



Configuring Radio Settings

This chapter describes how to configure basic radio settings for the Cisco wireless mobile interface card (WMIC).

Disabling and Enabling the Radio Interface

The WMIC radio is enabled by default. To disable the WMIC radio, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio <i>port</i>	Enters interface configuration mode for the radio interface.
Step 3	shutdown	Disables the radio port. Use the no form of the shutdown command to enable the radio port.
Step 4	end	Returns to privileged EXEC mode.

Configuring Radio Data Rates

Use the **speed dot11 interface** command to manage the data rates on wireless devices. At least one data rate must be set to **basic** on the wireless device.

Client devices are *required* to support at least one **basic** data rate or it will not be allowed to associate with the wireless device. For example, if the speed of the wireless device is set to basic-1.0, the client must support a 1.0 Mbps transmission rate or it will not be allowed to associate with the wireless device. If the speed of the wireless device is set to basic-1.0 and basic-6.0, the client must support a 1.0 Mbps or a 6.0 Mbps transmission rate or it will not be allowed to associate with the wireless device.

The wireless device always attempts to begin data transmission at the highest basic data rate. For example, if the client device supports both a 1.0 Mbps and a 6.0 Mbps transmission rate, both of the devices use the higher 6.0 Mbps transmission rate.

Client devices are *allowed* to transmit at other data rates, depending on the configuration. If the client device supports the basic data rate and due to environmental conditions, the wireless and client devices can transmit at a higher data rate, the devices will transmit unicast packets at the highest allowed data rate; multicast packets are always sent at the highest basic data rate.

If, due to environmental factors such as obstacles or interference, the wireless device cannot transmit data at the highest basic data rate, the wireless device steps the speed down to the highest rate that allows it to transmit data.

The wireless device can be configured to automatically transmit at the data rate that optimizes either the range of the transmission or the throughput of the data. Use the **range** keyword to optimize the wireless device for the best range. The wireless device sets the basic rate to **basic-1.0** and all other rates are allowed. Use the **throughput** keyword to optimize the wireless device for maximum data throughput. The wireless device sets all data rates to **basic**.

Table 3-1 shows the data rate settings for the **peed dot11 interface** command.

Table 3-1 Data Rates for Speed Command Keywords

Keyword	2.4 GHz 802.11b Radio	2.4 GHz 802.11g Radio	4.9 GHz at 5 MHz	4.9 GHz at 10 MHz	4.9 GHz at 20 MHz	5 GHz at 20 MHz
<i>rate</i>	basic-1.0, basic-2.0, basic-5.0, basic-11.0, 1.0, 2.0, 5.0, 11.0	basic-1.0, basic-2.0, basic-5.0, basic-11.0, basic-12.0, basic-18.0, basic-24.0, basic-36.0, basic-48.0, basic-54.0, 1.0, 2.0, 5.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0	basic-1.5, basic-2.25, basic-3.0, basic-4.5, basic-9.0, basic-12.0, basic-13.5, 1.5, 2.25, 3.0, 4.5, 9.0, 12.0, 13.5	basic-3.0, basic-4.5, basic-6.0, basic-9.0, basic-12.0, basic-18.0, basic-24.0, basic-27.0, 3.0, 4.5, 6.0, 9.0, 12.0, 18.0, 24.0, 27.0	basic-6.0, basic-9.0, basic-12.0, basic-18.0, basic-24.0, basic-36.0, basic-48.0, basic-54.0, 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, 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0
default	The default keyword is not supported on 802.11b radios.	basic-1.0, basic-2.0, basic-5.5, basic-11.0, 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0	basic-1.5, 2.25, basic-3.0, 4.5, basic-6.0, 9.0, 12.0, 13.5	basic-3.0, 4.5, basic-6.0, 9.0, basic-12.0, 18.0, 24.0, 27.0	basic-6.0, 9.0, basic-12.0, 18.0, basic-24.0, 36.0, 48.0, 54.0	basic-6.0, 9.0, basic-12.0, 18.0, basic-24.0, 36.0, 48.0, 54.0
range	basic-1.0, 2.0, 5.0, 11.0	basic-1.0, 2.0, 5.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0	basic-1.5, 2.25, 3.0, 4.5, 6.0, 9.0, 12.0, 13.5	basic-3.0, 4.5, 6.0, 9.0, 12.0, 18.0, 24.0, 27.0	basic-6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0	basic-6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0
no speed	basic-1.0, 2.0, 5.0, 11.0	basic-1.0, 2.0, 5.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0	basic-1.5, 2.25, 3.0, 4.5, 6.0, 9.0, 12.0, 13.5	basic-3.0, 4.5, 6.0, 9.0, 12.0, 18.0, 24.0, 27.0	basic-6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0	basic-6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0

Table 3-1 Data Rates for Speed Command Keywords (continued)

Keyword	2.4 GHz 802.11b Radio	2.4 GHz 802.11g Radio	4.9 GHz at 5 MHz	4.9 GHz at 10 MHz	4.9 GHz at 20 MHz	5 GHz at 20 MHz
throughput	basic-1.0, basic-2.0, basic-5.0, basic-11.0	basic-1.0, basic-2.0, basic-5.0, basic-11.0, basic-12.0, basic-18.0, basic-24.0, basic-36.0, basic-48.0, basic-54.0	basic-1.5, basic-2.25, basic-3.0, basic-4.5, basic-6.0, basic-9.0, basic- 12.0, basic-13.5	basic-3.0, basic-4.5, basic-6.0, basic-9.0, basic-12.0, basic-18.0, basic-24.0, basic-27.0	basic-6.0, basic-9.0, basic-12.0, basic-18.0, basic-24.0, basic-36.0, basic-48.0, basic-54.0	basic-6.0, basic-9.0, basic-12.0, basic-18.0, basic-24.0, basic-36.0, basic-48.0, basic-54.0
throughput ofdm		¹ Sets OFDM rates to basic-6.0, basic-9.0, basic-12.0, basic-18.0, basic-24.0, basic-36.0 and disables CCK data rates 1.0, 2.0, 5.5, 11.0.				

1. Disables 802.11b protection mechanisms, prevents 802.11b clients from associating to the wireless device, and maximizes throughput for 802.11g clients.

To set the speed of the wireless device, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio port	Enters interface configuration mode for the radio interface.
Step 3	speed	Enters one or more of the data rates or one of the keywords to set these data rates on the radio.
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves your entries to the startup configuration file.

Examples

This example sets a 5-GHz radio for **basic-6.0** and **basic-9.0** service only. Client devices must support **basic-6.0** and **basic-9.0** service or they will not be able to associate.

```
WMIC# configure terminal
WMIC(config)# interface dot11radio 1
WMIC(config-if)# speed basic-6.0 basic-9.0
WMIC(config-if)# end
```

This example sets a 2.4-GHz radio for **basic-1.0** service and allows all other data rates by using the **no** form of the command. Multicast packets are transmitted at 1 Mbps. Unicast packets are transmitted at the highest allowed data rate. Client devices must support **basic-1.0** service or they will not be able to associate.

```
WMIC# configure terminal
WMIC(config)# interface dot11radio 1
WMIC(config-if)# no speed
WMIC(config-if)# end
```

This example sets a 2.4-GHz radio to serve only 802.11g client devices by using the Irthogonal frequency division multiplexing (OFDM) keyword **throughput ofdm**.

```
WMIC# configure terminal
WMIC(config)# interface dot11radio 0
WMIC(config-if)# speed throughput ofdm
WMIC(config-if)# end
```

Verify Settings

Use the **show controller dot11radio** command to display the data rates for the **speed** command and the **default** keyword.

With the **speed** command set to the default value for a 2.4-GHz, 802.11g radio,

```
WMIC# configure terminal
WMIC(config)# interface dot11 0
WMIC(config-if)# speed default
WMIC(config-if)# end
```

the **show controller dot11radio** command displays the following:

```
WMIC# show controller dot11Radio0
interface Dot11Radio0
Radio Atheros AR5212, Address 000e.9bb0.7360, BBlock version
0.01, Software version 3.00.0 Serial number: FOC05120075
Carrier Set: Americas (US) Current Frequency: 2432 Mhz
Channel 5 Allowed Frequencies: 2412(1) 2417(2) 2422(3) 2427(4) 2432(5) 2437(6) 2442(7)
2447(8) 2452(9) 2457(10)
2462(11) Current CCK Power: 20 dBm Allowed CCK Power Levels: 7 10 13 15 17 20 Current OFDM
Power: 17 dBm Allowed OFDM
Power Levels: 7 10 13 15 17 ERP settings: protection mechanisms, non-ERP present.
Neighbors in non-erp mode:
0040.96a2.7d70 0013.5f0c.2961 000c.8548.d9b9 0007.50ca.6885
000e.9b91.cb82 0013.5f0c.2960 0013.5f0c.2962 000d.9701.212b
000e.9ba1.cba4 0014.a40b.b4f0
Current Rates: basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0
54.0
Allowed Rates: 1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Range Rates: basic-1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Throughput Rates: 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
```

With the **no speed** command set on a 2.4-GHz, 802.11g radio,

```
WMIC# configure terminal
WMIC(config)# interface dot11 0
WMIC(config-if)# no speed
WMIC(config-if)# end
```

the **show controller dot11radio** command displays the following:

```
WMIC# show controller dot11Radio 0
interface Dot11Radio0
Radio Atheros AR5212, Address 000e.9bb0.7360, BBlock version
0.01, Software version 3.00.0 Serial number: FOC05120075
Carrier Set: Americas (US) Current Frequency: 2432 Mhz
Channel 5 Allowed Frequencies: 2412(1) 2417(2) 2422(3)
2427(4) 2432(5) 2437(6) 2442(7) 2447(8) 2452(9) 2457(10)
2462(11) Current CCK Power: 20 dBm Allowed CCK Power Levels:
7 10 13 15 17 20 Current OFDM Power: 17 dBm Allowed OFDM
Power Levels: 7 10 13 15 17 ERP settings: protection
mechanisms, non-ERP present.
Neighbors in non-erp mode:
000e.9b91.cb82 000e.9ba1.cba4 0040.96a2.7d70 000d.9701.212b
0014.a40b.b4f0
Current Rates: basic-1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
Allowed Rates: 1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Range Rates: basic-1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Throughput Rates: 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
Default Rates: basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0
54.0
```

Configuring Radio Transmit Power (2.4-GHz Radio Only)

To set the transmit power on your WMIC radio, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio port	Enters interface configuration mode for the radio interface.
Step 3	power local { 1 5 10 20 30 50 100 maximum }	Sets the transmit power for the radio to one of the power levels allowed in your regulatory domain. All settings are in milliwatts (mW). The settings allowed in your regulatory domain might differ from the settings listed here. The 2.4-GHz (802.11b/g) radio transmits at up to 100 mW for the data rates of 1, 2, 5.5, and 11 Mbps. However, for the data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbss, the maximum transmit power for the 802.11g radio is 30 mW.
Step 4	power client { 1 5 10 20 30 50 100 maximum }	Sets the maximum power level allowed on client devices that associate to the WMIC 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 5	end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Saves 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 radio is the one that is least congested; at startup, the WMIC 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 to each bridge. The channel settings on your WMIC correspond to the frequencies available in your regulatory domain. See [Appendix B, “Channels and Antenna Settings,”](#) for the frequencies allowed in your domain.

IEEE 802.11g (2.4-GHz Band)

The radio operates on 11 channels from 2412 MHz 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 bridges that are close to each other.

To set the radio channel for the WMIC, follow these steps, beginning in privileged EXEC mode:

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

	Command	Purpose
Step 3	channel frequency least-congested	<p>Sets the default channel for the WMIC 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	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

4.9-GHz U.S. Public Safety Band

This band is available only in the U.S. The radio operates on 26 channels, 5-MHz wide, 10-MHz wide, or 20-MHz wide between 4940 MHz and 4990 MHz for the public safety community. To reduce interference between two consecutive intersections, use two different channels in line-of-sight, cascaded deployments.

The throughput is a minimum of:

- 4 Mbps half-duplex at 1-mile line-of-sight range for a 5-MHz-wide channel
- 8 Mbps half-duplex at 1-mile line-of-sight range for a 10-MHz-wide channel
- 16 Mbps half-duplex at 1-mile line-of-sight range for a 20-MHz-wide channel

To configure the channel spacing (the baseband) and center frequencies, use the **spacing** command:

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

	Command	Purpose
Step 3	channel { width { 5 10 20 } / <i>channel_number</i> <i>frequency</i> least_congested }	<p>Sets the channel width for C3202 WMIC 12.4(3g)JK to 5, 10, or 20 MHz.</p> <p>Sets the channel for the WMIC radio.</p> <p>To set channel spacing and specify a preferred channel based on a specified frequency for C3202 WMIC 12.3(2)JK, use the following command:</p> <p>spacing baseband-mhz [<i>channel center-frequency</i>]</p>
Step 4	end	Returns to privileged EXEC mode.

Table 3-2 lists the radio frequency data rates for the 4.9 GHz band:

Table 3-2 Radio Frequency Data Rates

Data Rate (Mbps)	Modulation on Sub-Carriers Based on OFDM	RMS Transmit Power (dBm)	Receiver Sensitivity (dBm)	Signal-to-Noise Ratio (dB)
20-MHz Channelization				
6	BPSK ¹	19	-94	4
9	BPSK	19	-93	4
12	QPSK ²	19	-92	6
18	QPSK	19	-91	6
24	16-QAM ³	19	-87	11
36	16-QAM	18	-84	11
48	64-QAM	16	-78	20
54	64-QAM	15	-75	20
10-MHz Channelization				
3	BPSK	19	-94	4
4.5	BPSK	19	-93	4
6	QPSK	19	-92	6
9	QPSK	19	-91	6
12	16-QAM	19	-87	11
18	16-QAM	18	-84	11
24	64-QAM	16	-78	20
27	64-QAM	15	-75	20
5-MHz Channelization				
1.5	BPSK	19	-97	4
2.25	BPSK	19	-96	4
3	QPSK	19	-95	6
4.5	QPSK	19	-94	6
6	16-QAM	19	-90	11

Table 3-2 *Radio Frequency Data Rates*

9	16-QAM	18	-87	11
12	64-QAM	16	-81	20
13.5	64-QAM	15	-78	20

1. Binary Phase Sift Keying
2. Quadrature Phase Shift Keying
3. Quadrature Amplitude Modulation

IEEE 802.11a (5.0-GHz Band)

The radio operates on 4 channels from 5250 MHz to 5350 MHz and on 11 channels from 5470 MHz to 5725 MHz. Each channel covers 20 MHz. For best performance, use channels that are not adjacent (such as 5260 and 5300) for bridges that are close to each other.

To configure the channel spacing (the baseband) and center frequencies, use the **spacing** command:

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


Command	Purpose
Step 3 channel <i>prefer_channel</i> [return-time <i>timeout_period</i>]	<p>Specifies the prefer channel for C3205 WMIC 12.4(3g)JK.</p> <p>(Optional) Specifies in 30-minute time units how long to wait before trying to return to the prefer channel after radar has been detected on the operating prefer channel.</p> <p>The minimum value is 1 time unit (30 minutes). The maximum value is 48 time units (1,440 minutes or 24 hours). The default value is 1 (30 minutes).</p> <p>To set the channel spacing to 5, 10, or 20 MHz for C3205 WMIC 12.3(2)JL, use the following command:</p> <pre>spacing {5 10 20} [channel {dfs {<i>channel_number</i> <i>frequency</i>} [return-time <i>timeout_period</i>]}]</pre> <p> Note The C3205 WMIC supports only 20-MHz spacing.</p> <p>You can also use this command to set the channel for the wireless device radio:</p> <ul style="list-style-type: none"> To let the Dynamic Frequency Selection (DFS) mechanism determine which channel to use, use the dfs option. For example: <pre>spacing {5 10 20} channel dfs</pre>or <pre>spacing {5 10 20}</pre> To specify a preferred channel, provide the channel number or frequency and, optionally, specify a timeout period for returning to the preferred channel. For example: <pre>spacing {5 10 20} channel {<i>channel_number</i> <i>frequency</i>} [return-time <i>timeout_period</i>]</pre> <p>For more information, see the “Configuring a Preferred Channel” section of the <i>Radio Channels and Transmit Frequencies</i> document.</p>
Step 4 end	Returns to privileged EXEC mode.

Table 3-3 lists the radio frequency data rates for the 5.0-GHz band.

Table 3-3 Radio Frequency Data Rates

Data Rate (Mbps)	Modulation on Sub-Carriers Based on OFDM	RMS Transmit Power (dBm)	Receiver Sensitivity (dBm)
20-MHz Channelization			
6	BPSK ¹	16	-85
9	BPSK	16	-85
12	QPSK ²	16	-85

Table 3-3 Radio Frequency Data Rates (continued)

18	QPSK	16	-82
24	16-QAM ³	16	-79
36	16-QAM	16	-76
48	64-QAM	14	-71
54	64-QAM	13	-69

1. Binary Phase Shift Keying
2. Quadrature Phase Shift Keying
3. Quadrature Amplitude Modulation

Enable and Disable World Mode (2.4-GHz Radio Only)

You can configure the WMIC to support 802.11d world mode or Cisco legacy world mode. When you enable world mode, the WMIC adds channel carrier set information to its beacon. Client devices with world mode enabled receive the carrier set information and automatically adjust their settings.

For example, a client device used mainly 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 WMIC is using 802.11d world mode or Cisco legacy world mode and automatically use the world mode that matches the mode used by the WMIC. World mode is disabled by default.

To enable world mode, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio port	Enters interface configuration mode for the radio interface.
Step 3	world-mode { legacy dot11d country_code code { both indoor outdoor } [roaming] }	Enables 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). The ISO website provides a list of ISO country codes. – After the country code, you must enter indoor, outdoor, or both to indicate the placement of the WMIC. • Enter the roaming option to cause the workgroup bridge to always passively scan for world mode. With roaming specified, the WMIC always obtains the country-specific list of frequency and output power level through passive scan before it performs active scan to associate with the Root device. • Enters the legacy option to enable Cisco legacy world mode.

	Command	Purpose
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves 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 (2.4-GHz Radio Only)

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

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

To disable short radio preambles, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio port	Enters interface configuration mode for the radio interface.
Step 3	no preamble-short	Disables short preambles and enables long preambles.
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves 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 that the WMIC uses to receive and transmit data:

- **Diversity**—This setting tells the WMIC to use the antenna that receives the best signal. This is the default setting for the C3201 and C3202 WMICs.
- **Right**—If you install a high-gain antenna on the right connector and no antenna on the left connector, you should use this setting for both receive and transmit. This is the default setting for the C3205 WMIC.





Note The most likely application for the C3205 WMIC will use only one antenna due to space constraints on the enclosure. If space is not an issue and you can use two antennas, use the diversity setting for better performance on the C3205 WMIC.

- **Left**—If you install a high-gain antenna on the left connector and no antenna on the right connector, use this setting for both receive and transmit.



Note The **antenna** commands are not available for bridges with a captive (internal) antenna.

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

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio port	Enters interface configuration mode for the radio interface.
Step 3	antenna receive { diversity left right }	Sets the receive antenna to diversity, left, or right.  Note For best performance when using one antenna, use the right setting. If using two antennas, use diversity.
Step 4	antenna transmit { diversity left right }	Sets the transmit antenna to diversity, left, or right.  Note For best performance when using one antenna, use the right setting. If using two antennas, use diversity.
Step 5	end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Saves your entries in the configuration file.



Note The **Antenna Gain (dB)** setting is disabled on the WMIC.

Configuring the Ethernet Encapsulation Transformation Method

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

- 802.1H—This method provides optimum performance for Cisco wireless products. This is the default setting.
- RFC 1042—Use this setting to ensure interoperability with non-Cisco wireless equipment. RFC 1042 does not provide the interoperability advantages of 802.1H, but it is used by other manufacturers of wireless equipment.

To configure the encapsulation transformation method, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio port	Enters interface configuration mode for the radio interface.
Step 3	payload-encapsulation RFC1042 dot1h	Sets the encapsulation transformation method to RFC1042 or 802.1h (dot1h , the default setting).
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves your entries in the configuration file.



Note

For best performance over your bridge links, adjust the contention window (CW) CW-min and CW-max settings to a value based on the number of non-root bridges associated to each root device.

Enabling and Disabling Concatenation (2.4-GHz Radio Only)

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

To enable concatenation and set the maximum length of concatenation, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio port	Enters 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	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring the Radio Distance Setting

Use the **distance** command to specify the distance from a root device to its clients (non-root bridges and/or workgroup bridges). The distance setting adjusts the time out values to account for the time required for radio signals for radio signals to travel from a root device to its clients (non-root bridges and/or workgroup bridges).

In installation mode, the default distance setting a 2.4-GHz WMIC is 99 km for maximum delay spread during antenna alignment. In other modes, the default distance setting is 0 km. Changing to a different mode sets the distance to the default distance.

If more than one non-root bridge (or workgroup bridge) communicates with the root device, enter the distance from the root device to the non-root bridge (or workgroup bridge) that is farthest away. Enter a value from 0 to 99 km for a 2.4- or 5.0-GHz WMIC or from 0 to 3 km for a 4.9-GHz WMIC. You do not need to adjust this setting on non-root bridges.

To configure the distance setting, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio port	Enters interface configuration mode for the radio interface.
Step 3	distance kilometers	Enters a distance setting from 0 to 99 km. Note The 802.11 standard was designed to support limited ranges (less than 1 km or 0.6 mi). To increase the supported range between a root device and its clients, you can specify the range to be supported (up to 99 km) on the dot11Radio interface.
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves 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 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; therefore, 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 workgroup bridge provides a wireless LAN connection for up to eight Ethernet-enabled devices. To configure the encapsulation transformation method, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio port	Enters interface configuration mode for the radio interface.
Step 3	infrastructure-client	Enables reliable multicast messages to workgroup bridges.
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves 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 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 3-17 for instructions on setting up protected ports.

Use bridge groups to enable and disable PSPF using command-line interface (CLI) commands on your access point. A detailed explanation of bridge groups and instructions for implementing them are provided 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/bcfpart1/bcftb.htm

To enable PSPF, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio <i>port</i>	Enters interface configuration mode for the radio interface.
Step 3	bridge-group <i>group</i> port-protected	Enables PSPF.
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves 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.

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

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

To disable protected port, use the **no switchport protected** command in global configuration mode.

For detailed information on protected ports and port blocking, see the “Configuring Port-Based Traffic Control” chapter in the *Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(12c)EA1*. Click the following link to browse to that configuration guide:

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

Configuring the Beacon Period

The beacon period is the amount of time between beacons in kilomicroseconds (Kusec). One Kusec equals 1,024 microseconds. The default beacon period is 100. To configure the beacon period, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio <i>port</i>	Enters interface configuration mode for the radio interface.
Step 3	beacon period <i>value</i>	Sets the beacon period. Enter a value between 20 and 4000.
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configure RTS Threshold and Retries

The RTS threshold determines the packet size at which the WMIC 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 WMIC, or in areas where the clients are far apart and can detect only the WMIC and not each other. You can enter a setting ranging from 0 to 2339 bytes.



Note

When concatenation is enabled for a 2.4-GHz WMIC, the RTS and fragment thresholds are set to 4000. Changing them to a lower value might degrade device performance. The 4.9-GHz WMIC does not support concatenation.

The maximum RTS retries is the maximum number of times that the WMIC issues an RTS before ceasing to attempt to send the packet over the radio. Enter a value from 1 to 128.

The default RTS threshold is 2312, and the default value for RTS retries is 32. To configure the RTS threshold and maximum RTS retries, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio <i>port</i>	Enters interface configuration mode for the radio interface.
Step 3	rts threshold <i>value</i>	Sets the RTS threshold. Enter an RTS threshold from 0 to 2339 for a 2.4-GHz WMIC or 0 to 4000 for a 4.9-GHz WMIC.
Step 4	rts retries <i>value</i>	Sets the maximum RTS retries. Enter a setting from 1 to 128.
Step 5	end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Use the **no** form of the command to reset the RTS threshold and maximum RTS retries to their default settings.

Configuring the Maximum Data Retries

The maximum data retries setting determines the number of attempts that the WMIC makes to send a packet before dropping the packet.

To configure the maximum data retries, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio <i>port</i>	Enters interface configuration mode for the radio interface.
Step 3	packet retries <i>value</i>	Sets the maximum data retries. Enter a setting from 1 to 128.
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Use the **no** form of the command to reset the minimum retries setting to the default.

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 there is a great deal of radio interference.



Note

When concatenation is enabled for the 2.4-GHz WMIC, the RTS and fragment thresholds are set to 4000. Changing them to a lower value may degrade performance. The 4.9-GHz WMIC does not support concatenation.

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

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio <i>port</i>	Enters interface configuration mode for the radio interface.
Step 3	fragment-threshold <i>value</i>	Sets the fragmentation threshold. Enter a setting from 256 to 4000 bytes.
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Use the **no** form of the command to reset the fragmentation threshold to its default value.

Setting the Root Parent Timeout Value

Use the **parent timeout** command to define the amount of time that a non-root bridge or workgroup bridge tries to associate with a parent access point. The command defines how long the 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. Use the **parent** command to set up the parent list. With the timeout disabled, the parent must come from the parent list.

To configure the root parent timeout value, follow these steps, beginning in privileged EXEC mode:

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

Use the **no** form of the command to reset the parent timeout to its default value.

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.



Caution

This command should not be used to configure a workgroup bridge or a non-root bridge for mobile application, because roaming time may be adversely affected. If the same devices are used for stationary applications the **parent** command can be configured.

To configure up to four parent MAC addresses, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio <i>port</i>	Enters interface configuration mode for the radio interface.
Step 3	parent <i>1-4 mac-address</i>	The value 1-4 specifies the parent root access point number. The mac-address specifies the MAC address of a parent access point (in xxxx.xxxx.xxxx format).
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Use the **no** form of the command to remove a parent from the list.

Performing a Carrier Busy Test

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

Enter this command to perform a carrier busy test in privileged EXEC mode:

```
dot 11 dot11Radio interface-number carrier busy
```

where *interface-number* is the dot11radio interface.

Use the **show dot11 carrier busy** command to redisplay the carrier busy test results.

