CHAPTER 5

# Configuring Radio Settings

This module describes how to configure radio settings for the wireless device in the following sections:

# Enabling the Radio Interface

The wireless device radios are disabled by default.

**Note** You must create a service set identifier (SSID) before you can enable the radio interface.

To enable the access point radio, follow these steps, beginning in privileged EXEC mode:

## SUMMARY STEPS

1. **configure terminal**
2. **dot11 ssid** *ssid*
3. **interface dot11radio** {**0**}
4. **ssid** *ssid*
5. **no shutdown**
6. **end**
7. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enters global configuration mode. |
| **Step 2** | **dot11 ssid** *ssid* | Enters the SSID.<br>**Note** The SSID consists of up to 32 alphanumeric characters. SSIDs are case sensitive. |
| **Step 3** | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 2.4-GHz and 802.11g/n 2.4-GHz radios are radio 0. |
| **Step 4** | **ssid** *ssid* | Assigns the SSID that you created in Step 2 to the appropriate radio interface. |
| **Step 5** | **no shutdown** | Enables the radio port. |
| **Step 6** | **end** | Returns to privileged EXEC mode. |
| **Step 7** | **copy running-config startup-config** | (Optional) Saves your entries in the configuration file. |

Use the **shutdown** command to disable the radio port.

# Configuring the Role in the Radio Network

The radio performs the following roles in the wireless network:

- Access point
- Access point (fallback to radio shutdown)
- Root bridge
- Non-root bridge
- Root bridge with wireless clients
- Non-root bridge without wireless clients

You can also configure a fallback role for root access points. The wireless device automatically assumes the fallback role when its Ethernet port is disabled or disconnected from the wired LAN. The default fallback role for Cisco ISR wireless devices is as follows:

**Shutdown**—the wireless device shuts down its radio and disassociates all client devices.

To set the wireless device's radio network role and fallback role, follow these steps, beginning in privileged EXEC mode:

## SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **station-role non-root** {**bridge | wireless-clients**} **root** {**access-point | ap-only | [bridge | wireless-clients] | [fallback | repeater | shutdown]**} **workgroup-bridge** {**multicast | mode** <*client | infrastructure*>**| universal** <*Ethernet client MAC address*>}
4. **end**
5. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enters global configuration mode. |
| Step 2 | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 2.4-GHz and 802.11g/n 2.4-GHz radios are radio 0. |
| Step 3 | **station-role**<br><br>**non-root** {**bridge** \| **wireless-clients**}<br><br>**root** {**access-point** \| **ap-only** \| **[bridge** \| **wireless-clients]** \| **[fallback** \| **repeater** \| **shutdown]**}<br><br>**workgroup-bridge** {**multicast** \| **mode** <*client* \| *infrastructure*>\| **universal** <*Ethernet client MAC address*>} | Sets the wireless device role.<br>• Sets the role to non-root bridge with or without wireless clients, to root access point or bridge, or to workgroup bridge.<br>**Note** The **bridge** mode radio supports point-to-point configuration only.<br>**Note** The **repeater** and **wireless-clients** commands are not supported on Cisco 860 Series and Cisco 880 Series Integrated Services Routers.<br>**Note** The **scanner** command is not supported on Cisco 860 Series and Cisco 880 Series Integrated Services Routers.<br>• The Ethernet port is shut down when any one of the radios is configured as a repeater. Only one radio per access point may be configured as a workgroup bridge or repeater. A workgroup bridge can have a maximum of 25 clients, presuming that no other wireless clients are associated to the root bridge or access point. |
| Step 4 | **end** | Returns to privileged EXEC mode. |
| Step 5 | **copy running-config startup-config** | (Optional) Saves your entries in the configuration file. |

**Note** When you enable the role of a device in the radio network as a bridge or workgroup bridge and enable the interface using the **no shut** command, the physical status and the software status of the interface will be up (ready) only if the device on the other end (access point or bridge) is up. Otherwise, only the physical status of the device will be up. The software status will be up when the device on the other end is configured and ready.

## Radio Tracking

You can configure the access point to track or monitor the status of one of its radios. If the tracked radio goes down or is disabled, the access point shuts down the other radio. If the tracked radio comes up, the access point enables the other radio.

To track radio 0, enter the following command:

```
# station-role root access-point fallback track d0 shutdown
```

## Fast Ethernet Tracking

You can configure the access point for fallback when its Ethernet port is disabled or disconnected from the wired LAN. For guidance on configuring the access point for Fast Ethernet tracking, see the "Configuring the Role in the Radio Network" section on page 5-3.

**Note** Fast Ethernet tracking does not support the repeater mode.

To configure the access point for Fast Ethernet tracking, enter the following command:

```
# station-role root access-point fallback track fa 0
```

## MAC-Address Tracking

You can configure the radio whose role is root access point to come up or go down by tracking a client access point, using its MAC address, on another radio. If the client disassociates from the access point, the root access point radio goes down. If the client reassociates to the access point, the root access point radio comes back up.

MAC-address tracking is most useful when the client is a non-root bridge access point connected to an upstream wired network.

For example, to track a client whose MAC address is 12:12:12:12:12:12, enter the following command:

```
# station-role root access-point fallback track mac-address 12:12:12:12:12:12 shutdown
```

# Configuring Radio Data Rates

You use the data rate settings to choose the data rates that the wireless device uses for data transmission. The rates are expressed in megabits per second (Mb/s). The wireless device always attempts to transmit at the highest data rate set to **basic**, also known as **required** on the browser-based interface. If there are obstacles or interference, the wireless device steps down to the highest rate that allows data transmission. You can set each data rate to one of three states:

- Basic (the GUI labels Basic rates as Required)—Allows transmission at this rate for all packets, both unicast and multicast. At least one of the data rates of the wireless device must be set to basic.
- Enabled—The wireless device transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to basic.
- Disabled—The wireless device 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 an access point to serve client devices operating at specific data rates. For example, to set the 2.4-GHz radio for 11 Mb/s service only, set the 11-Mb/s rate to **basic,** and set the other data rates to **disabled**. To set the wireless device to serve only client devices operating at 1 and 2 Mb/s, set 1 and 2 to **basic,** and set the rest of the data rates to **disabled**. To set the 2.4-GHz, 802.11g radio to serve only 802.11g client devices, set any orthogonal frequency division multiplexing (OFDM) data rate (6, 9, 12, 18, 24, 36, 48, 54) to **basic**. To set the 5-GHz radio for 54-Mb/s service only, set the 54-Mb/s rate to **basic,** and set the other data rates to **disabled**.

You can configure the wireless device to set the data rates automatically to optimize either the range or the throughput. When you enter **range** for the data rate setting, the wireless device sets the 1-Mb/s rate to **basic** and sets the other rates to **enabled**. The range setting allows the access point to extend the coverage area by compromising on the data rate. Therefore, if you have a client that cannot connect to the access point although other clients can, the client might not be within the coverage area of the access point. In such a case, using the range option will help extend the coverage area, and the client may be able to connect to the access point.

Typically, the trade-off is between throughput and range. When the signal degrades (possibly due to distance from the access point), the rates renegotiate in order to maintain the link (but at a lower data rate). A link that is configured for a higher throughput simply drops when the signal degrades enough that it no longer sustains a configured high data rate, or the link roams to another access point with sufficient coverage, if one is available. The balance between the two (throughput vs. range) is a design decision that must be made based on resources available to the wireless project, the type of traffic the users will be passing, the service level desired, and as always, the quality of the RF environment. When you enter **throughput** for the data rate setting, the wireless device sets all four data rates to **basic**.

**Note** When a wireless network has a mixed environment of 802.11b clients and 802.11g clients, make sure that data rates 1, 2, 5.5, and 11 Mb/s are set to **required** (**basic**) and that all other data rates are set to **enable**. The 802.11b adapters do not recognize the 54 Mb/s data rate and do not operate if data rates higher than 11 Mb/s are set to **required** on the connecting access point.

To configure the radio data rates, follow these steps, beginning in privileged EXEC mode:

## SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **speed**
4. **end**
5. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enters global configuration mode. |
| Step 2 | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 2.4-GHz and the 802.11g/n 2.4-GHz radios are radio 0. |

| | Command or Action | Purpose |
|---|---|---|
| Step 3 | **speed**<br><br>802.11b, 2.4-GHz radio:<br><br>{[**1.0**] [**11.0**] [**2.0**] [**5.5**] [**basic-1.0**] [**basic-11.0**] [**basic-2.0**] [**basic-5.5**] \| **range** \| **throughput**}<br><br>802.11g, 2.4-GHz radio:<br><br>{[**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** [**ofdm**] \| **default**}<br><br>802.11a 5-GHz radio:<br><br>{[**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** \| **ofdm-throughput** \| **default**}<br><br>802.11n 2.4-GHz radio:<br><br>{[**1.0**] [**11.0**] [**12.0**] [**18.0**] [**2.0**] [**24.0**] [**36.0**] [**48.0**] [**5.5**] [**54.0**] [**6.0**] [**9.0**] [**basic-1.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-5.5**] [**basic-54.0**] [**basic-6.0**] [**basic-9.0**] [**default**] [**m0-7**] [**m0.**] [**m1.**] [**m10.**] [**m11.**] [**m12.**] [**m13.**] [**m14.**] [**m15.**] [**m2.**] [**m3.**] [**m4.**] [**m5.**] [**m6.**] [**m7.**] [**m8-15**] [**m8.**] [**m9.**] [**ofdm**] [**only-ofdm**] \| **range** \| **throughput**} | Sets each data rate to **basic** or **enabled**, or enters **range** to optimize range or enters **throughput** to optimize throughput.<br><br>• (Optional) Enter **1.0**, **2.0**, **5.5**, and **11.0** to set these data rates to **enabled** on the 802.11b, 2.4-GHz radio.<br><br>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** on the 802.11g, 2.4-GHz radio.<br><br>Enter **6.0**, **9.0**, **12.0**, **18.0**, **24.0**, **36.0**, **48.0**, and **54.0** to set these data rates to **enabled** on the 5-GHz radio.<br><br>• (Optional) Enter **basic-1.0**, **basic-2.0**, **basic-5.5**, and **basic-11.0** to set these data rates to **basic** on the 802.11b, 2.4-GHz radio.<br><br>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** on the 802.11g, 2.4-GHz radio.<br><br>**Note** If the client must support the basic rate that you select, it cannot associate to the wireless device. If you select 12-Mb/s or higher for the basic data rate on the 802.11g radio, 802.11b client devices cannot associate to the wireless device 802.11g radio.<br><br>Enter **basic-6.0**, **basic-9.0**, **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** on the 5-GHz radio.<br><br>• (Optional) Enter **range** or **throughput** or **ofdm-throughput** (no ERP protection) to automatically optimize radio range or throughput. When you enter **range**, the wireless device sets the lowest data rate to **basic** and sets the other rates to **enabled**. When you enter **throughput**, the wireless device sets all data rates to **basic**.<br><br>(Optional) On the 802.11g radio, enter **speed throughput ofdm** to set all OFDM rates (6, 9, 12, 18, 24, 36, and 48) to **basic** (**required**) and to set all the CCK rates (1, 2, 5.5, and 11) to **disabled**. This setting disables 802.11b protection mechanisms and provides maximum throughput for 802.11g clients. However, it prevents 802.11b clients from associating to the access point.<br><br>• (Optional) Enter **default** to set the data rates to factory default settings (not supported on 802.11b radios).<br><br>On the 802.11g radio, the **default** option sets rates 1, 2, 5.5, and 11 to **basic**, and stes rates 6, 9, 12, 18, 24, 36, 48, and 54 to **enabled**. These rate settings allow both 802.11b and 802.11g client devices to associate to the wireless device 802.11g radio. |

| | Command or Action | Purpose |
|---|---|---|
| | **speed** (continued) | On the 5-GHz radio, the **default** option sets rates 6.0, 12.0, and 24.0 to **basic**, and stes rates 9.0, 18.0, 36.0, 48.0, and 54.0 to **enabled**.<br>On the 802.11g/n 2.4-GHz radio, the **default** option sets rates 1.0, 2.0, 5.5, and 11.0 to **enabled**.<br>On the 802.11g/n 5-GHz radio, the **default** option sets rates to 6.0, 12.0, and 24.0 to **enabled**.<br>The modulation coding scheme (MCS) index range for both 802.11g/n radios is 0 to 15. |
| **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 **speed** command to remove one or more data rates from the configuration. This example shows how to remove data rates **basic-2.0** and **basic-5.5** from the configuration:

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

# Configuring MCS Rates

Modulation coding scheme (MCS) is a specification of PHY parameters consisting of modulation order (binary phase shift keying [BPSK], quaternary phase shift keying [QPSK], 16-quadrature amplitude modulation [16-QAM], 64-QAM) and forward error correction (FEC) code rate (1/2, 2/3, 3/4, 5/6). MCS is used in the wireless device 802.11n radios, which define 32 symmetrical settings (8 per spatial stream):

- MCS 0–7
- MCS 8–15
- MCS 16–23
- MCS 24–31

The wireless device supports MCS 0–15. High-throughput clients support at least MCS 0–7.

MCS is an important setting because it provides for potentially greater throughput. High-throughput data rates are a function of *MCS*, *bandwidth*, and *guard interval*. The 802.11a, b, and g radios use 20-MHz channel widths. Table 5-1 shows potential data rated based on MCS, guard interval, and channel width.

***Table 5-1 Data Rates Based on MCS Settings, Guard Interval, and Channel Width***

| MCS Index | Guard Interval = 800 ns | | Guard Interval = 400 ns | |
|---|---|---|---|---|
| | 20-MHz Channel Width Data Rate (Mb/s) | 40-MHz Channel Width Data Rate (Mb/s) | 20-MHz Channel Width Data Rate (Mb/s) | 40-MHz Channel Width Data Rate (Mb/s) |
| 0 | 6.5 | 13.5 | 7 2/9 | 15 |
| 1 | 13 | 27 | 14 4/9 | 30 |

*Table 5-1 Data Rates Based on MCS Settings, Guard Interval, and Channel Width (continued)*

| MCS Index | Guard Interval = 800 ns | | Guard Interval = 400 ns | |
|---|---|---|---|---|
| 2 | 19.5 | 40.5 | 21 2/3 | 45 |
| 3 | 26 | 54 | 28 8/9 | 60 |
| 4 | 39 | 81 | 43 1/3 | 90 |
| 5 | 52 | 109 | 57 5/9 | 120 |
| 6 | 58.5 | 121.5 | 65 | 135 |
| 7 | 65 | 135 | 72 2/9 | 152.5 |
| 8 | 13 | 27 | 14 4/9 | 30 |
| 9 | 26 | 54 | 28 8/9 | 60 |
| 10 | 39 | 81 | 43 1/3 | 90 |
| 11 | 52 | 108 | 57 7/9 | 120 |
| 12 | 78 | 162 | 86 2/3 | 180 |
| 13 | 104 | 216 | 115 5/9 | 240 |
| 14 | 117 | 243 | 130 | 270 |
| 15 | 130 | 270 | 144 4/9 | 300 |
| The legacy rates are as follows: | | | | |
| 5 GHz: 6, 9, 12, 18, 24, 36, 48, and 54 Mb/s | | | | |
| 2.4 GHz: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mb/s | | | | |

MCS rates are configured using the **speed** command. The following example shows a **speed** setting for an 802.11g/n 2.4-GHz radio:

```
interface Dot11Radio0
    no ip address
    no ip route-cache
    !
    ssid 800test
    !
    speed basic-1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4.
    m8. m9. m10. m11. m12. m13. m14. m15.
```

# Configuring Radio Transmit Power

Radio transmit power is based on the type of radio or radios installed in your access point and the regulatory domain in which it operates.

To set the transmit power on access point radios, follow these steps, beginning in privileged EXEC mode:

## SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **power local**
4. **end**
5. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 2.4-GHz and the 802.11g/n 2.4-GHz radios are radio 0. |
| **Step 3** | **power local**<br>These options are available for the 2.4-GHz 802.11n radio (in dBm):<br>{**8** \| **9**\| **11** \| **14** \| **15** \| **17** \| **maximum**} | Sets the transmit power for the 2.4-GHz radio so that the power level is allowed in your regulatory domain. |
| **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 **power local** 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 wireless device. When a client device associates to the wireless device, the wireless device sends the maximum power level setting to the client.

**Note** Cisco AVVID documentation uses the term Dynamic Power Control (DPC) to refer to limiting the power level on associated client devices.

To specify a maximum allowed power setting on all client devices that associate to the wireless device, follow these steps, beginning in privileged EXEC mode:

## SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **power client**
4. **end**
5. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enters global configuration mode. |
| **Step 2** | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 2.4-GHz and 802.11g/n 2.4-GHz radios are radio 0. |
| **Step 3** | **power client**<br>These options are available for 802.11n 2.4-GHz clients (in dBm):<br>{**local** \| **8** \| **9** \| **11** \| **14** \| **15** \| **17** \| **maximum**} | Sets the maximum power level allowed on client devices that associate to the wireless device.<br>• Setting the power level to **local** sets the client power level to that of the access point.<br>• Setting the power level to **maximum** sets the client power to the allowed maximum.<br>**Note** The settings allowed in your regulatory domain might differ from the settings listed here. |
| **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 **power client** 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 wireless device radios is least congested. At startup, the wireless device scans for and selects the least-congested channel. For the 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 the wireless device correspond to the frequencies available in your regulatory domain. See the access point hardware installation guide for the frequencies allowed in your domain.

Each 2.4-GHz channel covers 22 MHz. Because the bands for channels 1, 6, and 11 do not overlap, you can set up multiple access points in the same vicinity without causing interference. The 802.11b and 802.11g 2.4-GHz radios use the same channels and frequencies.

The 5-GHz radio operates on 8 channels from 5180 to 5320 MHz, up to 27 channels from 5170 to 5850 MHz depending on regulatory domain. Each channel covers 20 MHz, and the bands for the channels overlap slightly. For best performance, use channels that are not adjacent (use channels 44 and 46, for example) for radios that are close to each other.

**Note** The presence of too many access points in the same vicinity can create radio congestion that can reduce throughput. A careful site survey can determine the best placement of access points for maximum radio coverage and throughput.

## 802.11n Channel Widths

The 802.11n standard allows both 20-MHz and 40-Mhz channel widths consisting of two contiguous non-overlapping channels (for example, 2.4-GHz channels 1 and 6).

One of the 20-MHz channels is called the *control channel*. Legacy clients and 20-MHz high-throughput clients use the control channel. Only beacons can be sent on this channel. The other 20-MHz channel is called the *extension channel.* The 40-MHz stations may use this channel and the control channel simultaneously.

A 40-MHz channel is specified as a channel and extension, such as 1,1. In this example, the control channel is channel 1 and the extension channel is above it.

To set the wireless device channel width, follow these steps, beginning in privileged EXEC mode:

### SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0** }
3. **channel** {*frequency* | **least-congested** | **width** [**20** | **40-above** | **40-below**] | **dfs**}
4. **end**
5. **copy running-config startup-config**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enters global configuration mode. |
| **Step 2** | **interface dot11radio** {**0** } | Enters interface configuration mode for the radio interface.<br>• The 802.11g/n 2.4-GHz radio is radio 0. |
| **Step 3** | **channel** {*frequency* \| **least-congested** \| **width** [**20** \| **40-above** \| **40-below**] \| **dfs**} | Sets the default channel for the wireless device radio.To search for the least-congested channel on startup, enter **least-congested**.<br>• Use the **width** option to specify a bandwidth to use. This option is available for the Cisco 800 series ISR wireless devices and consists of three available settings: **20**, **40-above**, and **40-below:**<br>– Choosing **20** sets the channel width to 20 MHz.<br>– Choosing **40-above** sets the channel width to 40 MHz with the extension channel above the control channel.<br>– Choosing **40-below** sets the channel width to 40 MHz with the extension channel below the control channel.<br>**Note** The **channel** command is disabled for 5-GHz radios that comply with European Union regulations on dynamic frequency selection (DFS). See the "Enabling and Disabling World Mode" section on page 5-14 for more information. |
| **Step 4** | **end** | Returns to privileged EXEC mode. |
| **Step 5** | **copy running-config startup-config** | (Optional) Saves your entries in the configuration file. |

# Enabling and Disabling World Mode

You can configure the wireless device to support 802.11d world mode, Cisco legacy world mode, or world mode roaming. When you enable world mode, the wireless device 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 detect whether the wireless device is using 802.11d or Cisco legacy world mode and automatically use the world mode that matches the mode used by the wireless device.

You can also configure world mode to be always on. In this configuration, the access point essentially roams between countries and changes its settings as required.

World mode is disabled by default.

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

## SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **world-mode** {**dot11d country_code** *code* {**both** | **indoor** | **outdoor**}| **world-mode roaming** | **legacy**}
4. **end**
5. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enters global configuration mode. |
| **Step 2** | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface. |
| **Step 3** | **world-mode** {**dot11d country_code** *code* {**both** \| **indoor** \| **outdoor**} \| **world-mode roaming** \| **legacy**} | Enables world mode.<br>• Enter the **dot11d** option to enable 802.11d world mode.<br>– 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.<br>– After the country code, you must enter **indoor**, **outdoor**, or **both** to indicate the placement of the wireless device.<br>• Enter the **legacy** option to enable Cisco legacy world mode.<br>• Enter the **world-mode roaming** option to place the access point in a continuous world mode configuration.<br>**Note** Aironet extensions must be enabled for legacy world mode operation, but Aironet extensions are not required for 802.11d world mode. Aironet extensions are enabled by default. |
| **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 **world-mode** command to disable world mode.

# 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 wireless device 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.
- Long—A long preamble ensures compatibility between the wireless device and all early models of Cisco Aironet Wireless LAN Adapters. If these client devices do not associate to the wireless devices, 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:

## SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0** }
3. **no preamble-short**
4. **end**
5. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enters global configuration mode. |
| **Step 2** | **interface dot11radio** {**0** } | Enters interface configuration mode for the 2.4-GHz 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 wireless device uses to receive and transmit data. There are three options for both the receive antenna and the transmit antenna:

- Gain—Sets the resultant antenna gain in decibels (dB).
- Diversity—This default setting tells the wireless device to use the antenna that receives the best signal. If the wireless device has two fixed (non-removable) antennas, you should use this setting for both receive and transmit.
- Right—If the wireless device has removable antennas and you install a high-gain antenna on the wireless device's right connector, you should use this setting for both receive and transmit. When you look at the wireless device's back panel, the right antenna is on the right.
- Left—If the wireless device has removable antennas and you install a high-gain antenna on the wireless device's left connector, you should use this setting for both receive and transmit. When you look at the wireless device's back panel, the left antenna is on the left.

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

## SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **gain** *dB*
4. **antenna receive** {**diversity | left | right**}
5. **end**
6. **copy running-config startup-config**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enters global configuration mode. |
| **Step 2** | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 802.11g/n 2.4-GHz radio is radio 0. |
| **Step 3** | **gain** *dB* | Specifies the resultant gain of the antenna attached to the device.<br>• Enter a value from –128 to 128 dB. If necessary, you can use a decimal in the value, such as 1.5.<br>**Note** The Cisco 860 and Cisco 880 ISRs are shipped with a fixed antenna that cannot be removed. The antenna gain cannot be configured on these models. |
| **Step 4** | **antenna receive** {**diversity** \| **left** \| **right**} | Sets the receive antenna to diversity, left, or right.<br>**Note** For best performance with two antennas, leave the receive antenna setting at the default setting, **diversity**. For one antenna, attach the antenna on the right and set the antenna for **right**. |
| **Step 5** | **end** | Returns to privileged EXEC mode. |
| **Step 6** | **copy running-config startup-config** | (Optional) Saves your entries in the configuration file. |

# Disabling and Enabling Aironet Extensions

By default, the wireless device 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 wireless device and associated client devices. Aironet extensions must be enabled to support these features:

- Load balancing—The wireless device uses Aironet extensions to direct client devices to an access point that provides the best connection to the network on the basis of such factors 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 the wireless device and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof.
- Cisco Key Integrity Protocol (CKIP)—Cisco's WEP key permutation technique is based on an early algorithm presented by the IEEE 802.11i security task group. The standards-based algorithm, Temporal Key Integrity Protocol (TKIP), does not require Aironet extensions to be enabled.
- World mode (legacy only)—Client devices with legacy world mode enabled receive carrier set information from the wireless device and adjust their settings automatically. Aironet extensions are not required for 802.11d world mode operation.
- Limiting the power level on associated client devices—When a client device associates to the wireless device, the wireless device 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 wireless device.

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

### SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **no dot11 extension aironet**
4. **end**
5. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enters global configuration mode. |
| **Step 2** | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>The 802.11g/n 2.4-GHz radio is radio 0. |
| **Step 3** | **no dot11 extension aironet** | Disables Aironet extensions. |
| **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 **dot11 extension aironet** command to enable Aironet extensions if they are disabled.

# Configuring the Ethernet Encapsulation Transformation Method

When the wireless device receives data packets that are not 802.3 packets, the wireless device 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.
- RFC 1042—Use this setting to ensure interoperability with non-Cisco wireless equipment. RFC1042 does not provide the interoperability advantages of 802.1H but is used by other manufacturers of wireless equipment.

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

### SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **payload-encapsulation** {**snap** | **dot1h**}
4. **end**
5. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enters global configuration mode. |
| **Step 2** | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 802.11g/n 2.4-GHz radio is radio 0. |
| **Step 3** | **payload-encapsulation** {**snap** \| **dot1h**} | Sets the encapsulation transformation method to RFC 1042 (**snap**) 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. |

# Enabling and Disabling Public Secure Packet Forwarding

Public Secure Packet Forwarding (PSPF) prevents client devices that are associated to an access point from inadvertently sharing files or communicating with other client devices that are associated to the access point. PSPF 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 the wireless devices are connected. See the "Configuring Protected Ports" section on page 5-21 for instructions on setting up protected ports.

To enable and disable PSPF using CLI commands on the wireless device, you use bridge groups. For a detailed explanation on bridge groups and instructions for implementing them, see the Configuring Transparent Bridging chapter of *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2* at the following link:

http://www.cisco.com/en/US/docs/ios/12_2/ibm/configuration/guide/bcftb_ps1835_TSD_Products_Configuration_Guide_Chapter.html

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

### SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **bridge-group** *group* **port-protected**
4. **end**
5. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enters global configuration mode. |
| Step 2 | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 802.11g/n 2.4-GHz radio is radio 0. |
| Step 3 | **bridge-group** *group* **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 **bridge group** command to disable PSPF.

# Configuring Protected Ports

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

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

### SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport protected**
4. **end**
5. **show interfaces** *interface-id* **switchport**
6. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enters global configuration mode. |
| Step 2 | **interface** *interface-id* | Enters interface configuration mode.<br>• Enter the type and number of the switch port interface to configure, such as **wlan-gigabitethernet0**. |
| Step 3 | **switchport protected** | Configures the interface to be a protected port. |
| Step 4 | **end** | Returns to privileged EXEC mode. |
| Step 5 | **show interfaces** *interface-id* **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.

For detailed information on protected ports and port blocking, see the "Configuring Port-Based Traffic Control" chapter in *Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(12c)EA1* at the following URL*:*

http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_12c_ea1/configuration/guide/3550scg.html

# Configuring the Beacon Period and the DTIM

The beacon period is the amount of time between access point beacons in kilomicroseconds (Kmicrosecs). One Kmicrosec 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 if the data beacon rate is set at 2, its default setting, then the wireless device sends a beacon containing a DTIM every 200 Kmicrosecs.

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

### SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **beacon period** *value*
4. **beacon dtim-period** *value*
5. **end**
6. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enters global configuration mode. |
| Step 2 | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 802.11g/n 2.4-GHz radio is radio 0. |
| Step 3 | **beacon period** *value* | Sets the beacon period.<br>• Enter a value in kilomicroseconds. |
| Step 4 | **beacon dtim-period** *value* | Sets the DTIM.<br>• Enter a value in kilomicroseconds. |
| Step 5 | **end** | Returns to privileged EXEC mode. |
| Step 6 | **copy running-config startup-config** | (Optional) Saves your entries in the configuration file. |

# Configure RTS Threshold and Retries

The request to send (RTS) threshold determines the packet size at which the wireless device issues an RTS before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the wireless device or in areas where the clients are far apart and can detect only the wireless device and not detect each other. You can enter a setting ranging from 0 to 2347 bytes.

The maximum RTS retries is the maximum number of times the wireless device 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 2347 for all access points and bridges, and the default maximum RTS retries setting is 32.

To configure the RTS threshold and maximum RTS retries, follow these steps, beginning in privileged EXEC mode:

### SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **rts threshold** *value*
4. **rts retries** *value*
5. **end**
6. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enters global configuration mode. |
| Step 2 | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 2.4-GHz and the 802.11g/n 2.4-GHz radios are radio 0. |
| Step 3 | **rts threshold** *value* | Sets the RTS threshold.<br>• Enter an RTS threshold from 0 to 2347. |
| Step 4 | **rts retries** *value* | Sets the maximum RTS retries.<br>• 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 **rts** command to reset the RTS settings to defaults.

# Configuring the Maximum Data Retries

The maximum data retries setting determines the number of attempts that the wireless device makes to send a packet before it drops the packet. The default setting is 32.

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

### SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **packet retries** *value*
4. **end**
5. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enters global configuration mode. |
| Step 2 | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 802.11g/n 2.4-GHz radio is radio 0. |
| Step 3 | **packet retries** *value* | Sets the maximum data retries.<br>• 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 **packet retries** command to reset the 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 communication is poor or where there is a great deal of radio interference. The default setting is 2346 bytes.

To configure the fragmentation threshold, follow these steps, beginning in privileged EXEC mode:

### SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **fragment-threshold** *value*
4. **end**
5. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enters global configuration mode. |
| **Step 2** | **interface dot11radio** {**0**} | Enters interface configuration mode for the radio interface.<br>• The 802.11g/n 2.4-GHz and 5-GHz radios are radio 0. |
| **Step 3** | **fragment-threshold** *value* | Sets the fragmentation threshold.<br>• Enter a setting from 256 to 2346 bytes for the 2.4-GHz radio.<br>• Enter a setting from 256 to 2346 bytes for the 5-GHz radio. |
| **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 **fragment-threshold** command to reset the setting to the default.

# Enabling Short Slot Time for 802.11g Radios

You can increase throughput on the 802.11g 2.4-GHz 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, which increases throughput. Backoff, 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.

Many 802.11g radios support short slot time, but some do not. When you enable short slot time, the wireless device uses the short slot time only when all clients associated to the 802.11g 2.4-GHz radio support short slot time.

Short slot time is supported only on the 802.11g 2.4-GHz radio. Short slot time is disabled by default.

In radio interface mode, enter the **short-slot-time** command to enable short slot time:

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

Use the **no** form of the **short-slot-time** command to disable short slot time.

# Performing a Carrier Busy Test

You can perform a carrier busy test to check the radio activity on wireless channels. During the carrier busy test, the wireless device drops all associations with wireless networking devices for 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.

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

# Configuring VoIP Packet Handling

You can improve the quality of VoIP packet handling per radio on access points by enhancing 802.11 MAC behavior for lower latency for the class of service (CoS) 5 (Video) and CoS 6 (Voice) user priorities.

To configure VoIP packet handling on an access point, follow these steps:

**Step 1** Using a browser, log in to the access point.

**Step 2** Click **Services** in the task menu on the left side of the web-browser interface.

**Step 3** When the list of Services expands, click **Stream**.

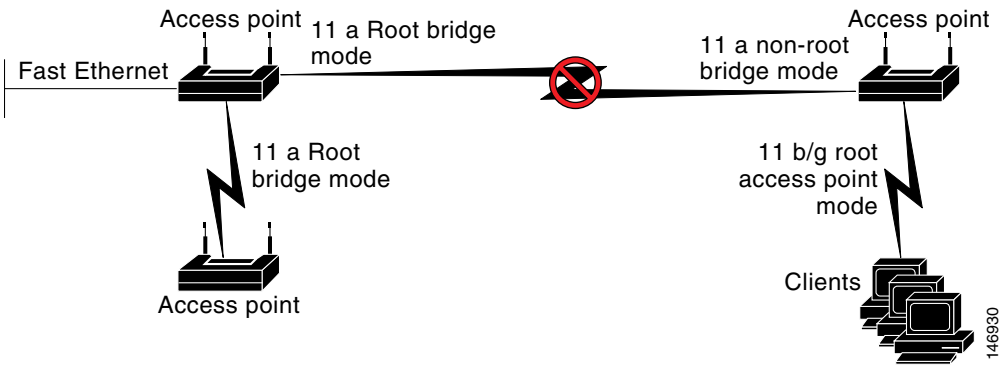
The Stream page appears.

**Step 4** Click the tab for the radio to configure.

**Step 5** For both CoS 5 (Video) and CoS 6 (Voice) user priorities, choose Low Latency from the Packet Handling drop-down menu, and enter a value for maximum retries for packet discard in the corresponding field.

The default value for maximum retries is 3 for the Low Latency setting (Figure 5-1). This value indicates how many times the access point will try to retrieve a lost packet before discarding it.

*Figure 5-1 Packet Handling Configuration*




**Note** You may also configure the CoS 4 (Controlled Load) user priority and its maximum retries value.

**Step 6** Click **Apply**.

You can also configure VoIP packet handling using the CLI. For a list of Cisco IOS commands for configuring VoIP packet handling using the CLI, consult *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.