Configuring Radio Settings

This chapter describes how to configure radio settings for the wireless device. This chapter includes these sections:

Enabling the Radio Interface

The wireless device radios are disabled by default.

Note In Cisco IOS Release 12.4 there is no default SSID. You must create a Radio Service Set Identifier (SSID) before you can enable the radio interface.

Beginning in privileged EXEC mode, follow these steps to enable the wireless device radio:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**ssid**	Enter the SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.
Step 4	**no shutdown**	Enable the radio port.
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 **shutdown** command to disable the radio port.

Roles in Radio Network

You can configure the following roles in a radio network:

- Network or Fallback Role
- Universal Client Mode

Table 2-1 shows the role in the radio network for each device.

Table 2-1 Device Role in Radio Network Configuration

Role in Radio Network	Cisco 800 series ISRs	Cisco 1800 series ISRs	Cisco 1841 series	Cisco 2800 series ISRs	Cisco 3800 series ISRs
Root access point	X	X	X	X	X
Root bridge with or without clients	–	–	X	X	X
Non-root bridge without clients	–	–	X	X	X
Universal client mode	X	X	X	X	X
Support of Workgroup bridge clients	X	X	X	X	X

Configuring Network or Fallback Role

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. Thefallback role is Shutdown—the wireless device shuts down its radio and disassociates all client devices.

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**station-role** **non-root {bridge | return}** **root {fallback | repeater | wireless clients | shutdown]}**	Sets the wireless device role to universal client mode. • Set the role to non-root bridge with or without wireless clients, repeater access point, root access point or bridge, scanner, or workgroup bridge. • The bridge mode radio supports point-to-point configuration only. • 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. • The **dot11radio 0|1 antenna-alignment** command is available when the access point is configured as a repeater. • Spanning Tree Protocol (STP) is configurable on Cisco ISR series access points in bridge modes. • (Optional) Select the root access point's fallback role. If the wireless device's Ethernet port is disabled or disconnected from the wired LAN, the wireless device can either shut down its radio port or become a repeater access point associated to any nearby root access point.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Bridge Features Not Supported

The following features are not supported when a Cisco ISR series access point is configured as a bridge:

- Clear Channel Assessment (CCA)
- Interoperability with 1400 series bridge
- Concatenation
- Install mode
- EtherChannel and PageP configuration on switch

For root and non-root bridging mode operations, only bridge-group mode using BVI interface is supported. Routing mode is not supported for root and non-root bridging operations.

Sample Bridging Configuration

The following is a sample of a Root Bridge Configuration:

```
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 20.0.0.1 auth-port 1812 acct-port 1813
!
aaa authentication login eap_methods group rad_eap
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
dot11 ssid airlink2-bridge
   vlan 1
   authentication open
   authentication key-management wpa
   wpa-psk ascii 0 12345678
!
dot11 priority-map avvid
ip cef
!
!
no ip domain lookup
!
!
bridge irb
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
```

```
 ip address 30.0.0.1 255.0.0.0
 duplex auto
 speed auto
!
interface Dot11Radio0/0/0
 no ip address
 !
 encryption vlan 1 mode ciphers tkip
 !
 ssid airlink2-bridge
 !
 speed 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
 station-role root bridge
!
interface Dot11Radio0/0/0.1
 encapsulation dot1Q 1 native
 no snmp trap link-status
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0/0/1
 no ip address
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
!
interface BVI1
 ip address 20.0.0.1 255.0.0.0
!
ip route 0.0.0.0 0.0.0.0 20.0.0.5
!
!
ip http server
no ip http secure-server
!
!
radius-server local
  nas 20.0.0.1 key 0 wireless
  user non-root nthash 0 3741A4EE66E1AA56CD8B3A9038580DC9
!
radius-server host 20.0.0.1 auth-port 1812 acct-port 1813 key wireless
!
control-plane
!
bridge 1 route ip
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end
```

The following is a sample of Non-Root Bridge Configuration:

```
no aaa new-model
```

```
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
dot11 ssid airlink2-bridge
   vlan 1
   authentication open
   authentication key-management wpa
   wpa-psk ascii 0 12345678
!
dot11 priority-map avvid
ip cef
!
!
bridge irb
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0/1/0
 no ip address
 !
 encryption vlan 1 mode ciphers tkip
 !
 ssid airlink2-bridge
 !
 speed 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
 station-role non-root bridge
!
interface Dot11Radio0/1/0.1
 encapsulation dot1Q 1 native
 no snmp trap link-status
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 20.0.0.5 255.0.0.0
!
ip route 0.0.0.0 0.0.0.0 20.0.0.1
!
!
ip http server
no ip http secure-server
!
!
control-plane
!
bridge 1 route ip
!
!
```

```
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end
```

Universal Client Mode

Universal client mode is a wireless radio station role that allows the radio to act as a wireless client to another access point or repeater. This feature is exclusive to the integrated radio running in the Cisco 870, 1800, 2800, and 3800 Integrated Services Routers. It operates differently from the workgroup bridge and non-root bridge modes that are supported on other Cisco wireless devices such as the Cisco AP 1200.

Universal client mode has the following features and limitations:

- You can configure universal client mode on the main **dot11radio** interface only, sub-interfaces are not supported.
- Universal client can associate to access points with radio VLANs.
- Layer-3 routing is supported over the radio interface. However, there is no support for L2-bridging. The user cannot configure a dot11radio interface with a bridge-group when in universal client mode.
- SSIDs are required to be configured on the dot11 interface operating as a universal client; association to an access point running in guest-mode is not supported.
- The universal client can associate to Cisco access points, 3rd party access points, and repeaters. It cannot associate to Cisco root bridges or Cisco workgroup bridges.

Configuring Universal Client Mode

You can configure universal client mode in Cisco ISR series by setting the radio interface station-role to non-root. This is different from configuring the **dot11radio** interface to operate in non-root bridge mode, which requires specifying the word bridge at the end of the command, ex: "**station-role non-root bridge**".

Note In other Cisco wireless products such as the Cisco AP1232, **station-role non-root** operates the same as **station-role non-root bridge**. On the ISRs, the two commands are different: **station-role non-root** is considered the universal client mode and **station-role non-root bridge** is considered the non-root bridge mode.

Example using Cisco 2801 series router:

```
c2801#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
c2801(config)#interface Dot11Radio0/1/0
```

```
c2801(config-if)#station-role ?
  non-root  Non-root (bridge)
  root      Root access point or bridge

c2801(config-if)#station-role non-root ?
  bridge  Bridge non-rootThis CLI enables non-root bridge mode.
  <cr>      This CLI enables universal client mode
```

DHCP

IP DHCP addressing is supported in the Dot11Radio interface configured in universal client mode. The following is an example of Dot11Radio configured with "ip address dhcp":

```
dot11 ssid test10
   authentication open
!
interface Dot11Radio0/1/0
 ip address dhcp
 !
 ssid test10
 !
 speed 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
 station-role non-root
```

Issuing a "show ip interface brief" will show the Virtual-Dot11Radio interface getting the IP address from the DHCP server.

```
c2801_uc#sh ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
Dot11Radio0/1/0            unassigned      YES DHCP   up                    up
Dot11Radio0/1/1            unassigned      YES NVRAM  administratively down down
Virtual-Dot11Radio0        200.1.1.2       YES DHCP   up                    up
c2801_uc#
```

NAT (Network Address Translation):

NAT translation takes place if you overload the interface which has an ip address. In the case of universal client, the virtual-interface has the ip address obtained from the DHCP. Hence we require to overload the virtual interface to aid NAT translation.

Note NAT fails to translate with a DHCP address on the **dot11** interface running in universal client mode.

The following configuration is supported on NAT:

```
ip nat inside source list 1 interface Virtual-Dot11Radio0 overload
```

The following is an example of a NAT configuration on a Cisco 1803 ISR:

```
C1803W_UC#
C1803W_UC#sh run
Building configuration...

Current configuration : 2189 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname C1803W_UC
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
no logging console
!
no aaa new-model
!
resource policy
!
!
dot11 ssid hurricane
   authentication open
   authentication key-management wpa
   wpa-psk ascii 0 allyouneedislove
!
dot11 ssid tsunami
   authentication open
   guest-mode
!
dot11 priority-map avvid
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 100.1.1.1
!
ip dhcp pool jimmy
   network 100.1.1.0 255.255.255.0
   default-router 100.1.1.1
!
!
!
!
!
!
controller DSL 0
 line-term cpe
!
!
bridge irb
!
interface Dot11Radio0
 ip address 100.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 no ip route-cache cef
 no ip route-cache
 !
 ssid tsunami
 !
 speed 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
 station-role root
 rts threshold 2312
 no cdp enable
!
interface Dot11Radio1
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
```

```
 !
 encryption mode ciphers tkip
 !
 ssid hurricane
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role non-root
!
End
```

Configuring Radio Data Rates

You use the data rate settings to choose the data rates the wireless device uses for data transmission. The rates are expressed in megabits per second. The wireless device 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 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 wireless device's data rates 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 megabits per second (Mbps) service only, set the 11-Mbps 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 Mbps, 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 Mbps service only, set the 54-Mbps 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 Mbps rate to basic and the other rates to **enabled**. When you enter **throughput** for the data rate setting, the wireless device sets all four data rates to **basic**.

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

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

	Command	Purpose
Step 3	**speed** These options are available for the 802.11b, 2.4-GHz radio: {[**1.0**] [**11.0**] [**2.0**] [**5.5**] [**basic-1.0**] [**basic-11.0**] [**basic-2.0**] [**basic-5.5**] | **range** | **throughput**} These options are available for the 802.11g, 2.4-GHz radio: {[**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** } These options are available for the 5-GHz radio: {[**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** |**default** }	Set each data rate to **basic** or **enabled**, or enter **range** to optimize range or **throughput** to optimize throughput. • (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. 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. 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. • (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. 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. **Note** The client must support the basic rate that you select or it cannot associate to the wireless device. 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 wireless device's 802.11g radio. 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. • (Optional) Enter **range** or **throughput** to automatically optimize radio range or throughput. When you enter **range**, the wireless device sets the lowest data rate to basic and the other rates to **enabled**. When you enter **throughput**, the wireless device sets all data rates to **basic**. (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 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. • (Optional) Enter **default** to set the data rates to factory default settings (not supported on 802.11b radios). On the 802.11g radio, the **default** option sets rates 1, 2, 5.5, and 11 to basic, and 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's 802.11g radio. On the 5-GHz radio, the **default** option sets rates 6.0, 12.0, and 24.0 to basic, and rates 9.0, 18.0, 36.0, 48.0, and 54.0 to enabled.

	Command	Purpose
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 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:

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

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 determine what transmit power is available for your access point and which regulatory domain it operates in, refer to the hardware installation guide for that device. hardware installation guides are available at cisco.com. Follow these steps to view and download them:

Step 1 Browse to http://www.cisco.com.

Step 2 Click **Technical Support & Documentation**. A small window appears containing a list of technical support links.

Step 3 Click **Technical Support & Documentation**. The Technical Support and Documentation page appears.

Step 4 In the Documentation & Tools section, choose **Wireless**. The Wireless Support Resources page appears.

Step 5 In the Wireless LAN Access section, choose the device you are working with. An introduction page for the device appears.

Step 6 In the Install and Upgrade section, choose **Install and Upgrade Guides**. The Install and Upgrade Guides page for the device appears.

Step 7 Choose the hardware installation guide for the device. The home page for the guide appears.

Step 8 In the left frame, click **Channels and Antenna Settings**.

Table 2-2 shows the relationship between mW and dBm.

Table 2-2 Translation between mW and dBm

dBm	-1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
mW	1	2	3	4	5	6	8	10	12	15	20	25	30	40	50	60	80	100	125	150	200	250

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**power local** power settings should be: {**3** | **4** | **5** | **6** | **7** | **10** | **13** | **15** | **17** | **18** | **20** | **maximum**}	Set the transmit power for the 802.11g, 2.4-GHz radio to one of the power levels allowed in your regulatory domain. All settings are in mW. On the 2.4-GHz, 802.11g radio, 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** See the hardware installation guide for your access point to determine the power settings for your regulatory domain. **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 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 power command to return the power setting to **maximum**, the default setting.

Limiting the Power Level for Associated Client Devices

You can also limit the power level on client devices that associate to the 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 (DTPC) to refer to limiting the power level on associated client devices.

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

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

	Command	Purpose
Step 3	**power client** These options are available for 802.11b, 2.4-GHz clients (in mW): { **1** | **5** | **20** | **30** | **50** | **100** | **maximum**} These options are available for 802.11g, 2.4-GHz clients (in mW): { **1** | **5** | **10** | **20** | **30** | **50** | **100** | **maximum**} These options are available for 5-GHz clients (in mW): { **5** | **10** | **20** | **40** | **maximum** }	Set the maximum power level allowed on client devices that associate to the wireless device. **Note** The settings allowed in your regulatory domain might differ from the settings listed here.
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 client power command to disable the maximum power level for associated clients.

Note Access Point extensions must be enabled to limit the power level on associated client devices. Access Point 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's hardware installation guide for the frequencies allowed in your domain.

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

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

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

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**channel** *frequency* | **least-congested**	Set the default channel for the wireless device radio. Table 2-3 through Table 2-6 show the available channels and frequencies for all radios. To search for the least-congested channel on startup, enter **least-congested**. **Note** The **channel** command is disabled for 5-GHz radios that comply with European Union regulations on dynamic frequency selection (DFS). See the "DFS Automatically Enabled on Some 5-GHz Radio Channels" section on page 2-18 for more information.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Table 2-3 shows the available channels and frequencies for the IEEE 802.11b 2.4-GHz radio.

Table 2-3 Channels and Frequencies for 802.11b 2.4 GHz Radio

Channel Identifier	Center Frequency (MHz)	Regulatory Domains			
		Americas (–A)	China (–C)	EMEA (–E)	Japan (–J)
1	2412	X	X	X	X
2	2417	X	X	X	X
3	2422	X	X	X	X
4	2427	X	X	X	X
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	X	X
11	2462	X	X	X	X
12	2467	–	–	X	X
13	2472	–	–	X	X
14	2484	–	–	–	–

Table 2-4 shows the available frequencies for the 802.11g 2.4 GHz radio.

Table 2-4 Channels and Available Frequencies for 802.11g 2.4 GHz Radio

Channel Identifier	Center Frequency (MHz)	Regulatory Domains					
		Americas (–A)		EMEA (–E)		Japan (–J)	
		CCK	OFDM	CCK	OFDM	CCK	OFDM
1	2412	X	X	X	X	X	X
2	2417	X	X	X	X	X	X
3	2422	X	X	X	X	X	X
4	2427	X	X	X	X	X	X
5	2432	X	X	X	X	X	X
6	2437	X	X	X	X	X	X
7	2442	X	X	X	X	X	X
8	2447	X	X	X	X	X	X
9	2452	X	X	X	X	X	X
10	2457	X	X	X	X	X	X
11	2462	X	X	X	X	X	X
12	2467	–	–	X	X	X	X
13	2472	–	–	X	X	X	X
14	2484	–	–	–	–	X	–

Table 2-5 shows the available channels and frequencies for the RM20A IEEE 802.11a radio

Table 2-5 Channels and Available Frequencies for the 802.11a Radio

Channel Identifier	Center Frequency (MHz)	Regulatory Domains					
		Americas (–A)		EMEA (–N)		Japan (–P)	
		CCK	OFDM	CCK	OFDM	CCK	OFDM
1	2412	X	X	X	X	X	X
2	2417	X	X	X	X	X	X
3	2422	X	X	X	X	X	X
4	2427	X	X	X	X	X	X
5	2432	X	X	X	X	X	X
6	2437	X	X	X	X	X	X
7	2442	X	X	X	X	X	X
8	2447	X	X	X	X	X	X
9	2452	X	X	X	X	X	X
10	2457	X	X	X	X	X	X
11	2462	X	X	X	X	X	X
12	2467	–	–	X	X	X	X

Channel Identifier	Center Frequency (MHz)	Regulatory Domains					
		Americas (–A)		EMEA (–N)		Japan (–P)	
		CCK	OFDM	CCK	OFDM	CCK	OFDM
13	2472	–	–	X	X	X	X
14	2484	–	–	–	–	X	–

Table 2-6 shows the available frequencies for the RM21A and RM22A IEEE 802.11a 5-GHz radios.

Note The frequencies allowed in your regulatory domain might differ from the frequencies listed here.

Table 2-6 Channels and Available Frequencies for the 802.11a 5-GHz Radios

Channel ID	Center Freq (MHz)	Americas (–B)	China (–C)	EMEA (–E)	New Zealand, Australia (–N)	Japan (–P)	–
34	5170	–	–	–	–	–	–
36	5180	x	–	x	x	x	–
38	5190	–	–	–	–	–	–
40	5200	x	–	x	x	x	–
42	5210	–	–	–	–	–	–
44	5220	x	–	x	x	x	–
46	5230	–	–	–	–	–	–
48	5240	x	–	x	x	x	–
52	5260	–	–	x	x	x	–
56	5280	–	–	x	x	x	–
60	5300	–	–	x	x	x	–
64	5320	–	–	x	x	x	–
100	5500	–	–	x	–	–	–
104	5520	–	–	x	–	–	–
108	5540	–	–	x	–	–	–
112	5560	–	–	x	–	–	–
116	5580	–	–	x	–	–	–
120	5600	–	–	–	–	–	–
124	5620	–	–	–	–	–	–
128	5640	–	–	–	–	–	–
132	5660	–	–	–	–	–	–
136	5680	–	–	x	–	–	–
140	5700	–	–	x	–	–	–
149	5745	x	x	–	x	–	–
153	5765	x	x	–	x	–	–
157	5785	x	x	–	x	–	–

Channel ID	Center Freq (MHz)	Americas (–B)	China (–C)	EMEA (–E)	New Zealand, Australia (–N)	Japan (–P)	–
161	5805	x	x	–	x	–	–
165	5825	–	–	x	–	–	–

DFS Automatically Enabled on Some 5-GHz Radio Channels

Access points with 5-GHz radios configured at the factory for use in Europe now comply with regulations that require radio devices to use Dynamic Frequency Selection (DFS) to detect radar signals and avoid interfering with them. Radios configured for use in other regulatory domains do not use DFS.

When a DFS-enabled 5-GHz radio operates on one of the 15 channels listed in Table 2-7, the access point automatically uses DFS to set the operating frequency.

Note You cannot manually select a channel for DFS-enabled 5-GHz radios.

Table 2-7 DFS Automatically Enabled on these 5-GHz Channels

5-GHz Channels on Which DFS is Automatically Enabled		
52 (5260 MHz)	104 (5520 MHz)	124 (5620 MHz)
56 (5280 MHz)	108 (5540 MHz)	128 (5640 MHz)
60 (5300 MHz)	112 (5560 MHz)	132 (5660 MHz)
64 (5320 MHz)	116 (5580 MHz)	136 (5680 MHz)
100 (5500 MHz)	120 (5600 MHz)	140 (5700 MHz)

When DFS is enabled, the access point monitors its operating frequency for radar signals. If it detects radar signals on the channel, the access point takes these steps:

- Blocks new transmissions on the channel.
- Flushes the power-save client queues.
- Broadcasts an 802.11h channel-switch announcement.
- Disassociates remaining client devices.
- Randomly selects a different 5-GHz channel.
- If the channel selected is one of the channels in Table 2-7, scans the new channel for radar signals for 60 seconds.
- If there are no radar signals on the new channel, enables beacons and accepts client associations.

Note The maximum legal transmit power is greater for some 5-GHz channels than for others. When it randomly selects a 5-GHz channel on which power is restricted, the access point automatically reduces transmit power to comply with power limits for that channel.

Note We recommend that you use the **world-mode dot11d** *country-code* configuration interface command to configure a country code on DFS-enabled radios. The IEEE 802.11h protocol requires access points to include the country information element (IE) in beacons and probe responses. By default, however, the country code in the IE is blank. You use the **world-mode** command to populate the country code IE.

Confirming that DFS is Enabled

Use the **show controller dot11radio1** command to confirm that DFS is enabled. This example shows a line from the output for the show controller command for a channel on which DFS is enabled:

```
Current Frequency: 5300 MHz  Channel 60 (DFS enabled)
```

Blocking Channels from DFS Selection

If your regulatory domain limits the channels that you can use in specific locations--for example, indoors or outdoors--you can block groups of channels to prevent the access point from selecting them when DFS is enabled. Use this configuration interface command to block groups of channels from DFS selection:

[**no**] **dfs band** [**1**] [**2**] [**3**] [**4**] **block**

The 1, 2, 3, and 4 options designate blocks of channels:

- **1**—Specifies frequencies 5.150 to 5.250 GHz. This group of frequencies is also known as the UNII-1 band.
- **2**—Specifies frequencies 5.250 to 5.350 GHz. This group of frequencies is also known as the UNII-2 band.
- **3**—Specifies frequencies 5.470 to 5.725 GHz.
- **4**—Specifies frequencies 5.725 to 5.825 GHz. This group of frequencies is also known as the UNII-3 band.

This example shows how to prevent the access point from selecting frequencies 5.150 to 5.350 GHz during DFS:

```
router(config-if)# dfs band 1 2 block
```

This example shows how to unblock frequencies 5.150 to 5.350 for DFS:

```
router(config-if)# no dfs band 1 2 block
```

This example shows how to unblock all frequencies for DFS:

```
router(config-if)# no dfs band block
```

Enabling and Disabling World Mode

You can configure the wireless device to support 802.11d world mode or Cisco legacy world mode. 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 running firmware version 5.30.17 or later detect whether the wireless device is using 802.11d or Cisco legacy world mode and automatically use world mode that matches the mode used by the wireless device. World mode is disabled by default.

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1**}	Enter interface configuration mode for the radio interface.
Step 3	**world-mode dot11d country_code** *code* { **both** | **indoor** | **outdoor** } | **legacy**	Enable world mode. • Enter the **dot11d** option to enable 802.11d world mode. – 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 wireless device. • Enter the **legacy** option to enable Cisco legacy world mode. **Note** Access Point extensions must be enabled for legacy world mode operation, but Access Point extensions are not required for 802.11d world mode. Access Point extensions are enabled by default.
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 world mode.

Enabling and Disabling 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. Cisco Access Point Wireless LAN Client Adapters support short preambles.
- Long—A long preamble ensures compatibility between the wireless device and all early models of Cisco Access Point Wireless LAN Adapters (PC4800 and PC4800A). 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.

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 2.4-GHz 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 wireless device uses to receive and transmit data. There are three options for both the receive and the transmit antenna:

- 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.

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**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**. **Note** The Cisco 850 series routers do not support diversity.

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

Disabling and Enabling Access Point Extensions

By default, the wireless device uses Cisco Access Point extensions to detect the capabilities of Cisco Access Point client devices and to support features that require specific interaction between the wireless device and associated client devices. Cisco Access Point extensions must be enabled to support these features:

- Load balancing—The wireless device uses Access Point 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 wireless device and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof.
- World mode (legacy only)—Client devices with legacy world mode enabled receive carrier set information from the wireless device and adjust their settings automatically. Access Point 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 Access Point extensions disables the features listed above, but it sometimes improves the ability of other companies devices to associate to the wireless device.

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**no dot11 extension aironet**	Disable Access Point extensions.
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 **dot11 extension aironet** command to enable Access Point 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 using an encapsulation transformation method. These are the two transformation methods:

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

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** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**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.

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 Access Point Workgroup Bridges that are associated to the wireless device. The default setting, **disabled**, reduces the reliability of multicast delivery to allow more workgroup bridges to associate to the wireless device.

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 wireless device 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 wireless device. To increase beyond 20 the number of workgroup bridges that can maintain a radio link to the wireless device, the wireless device must reduce the delivery reliability of multicast packets to workgroup bridges. With reduced reliability, the wireless device cannot confirm whether multicast packets reach the intended workgroup bridge, so workgroup bridges at the edge of the wireless device'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 wireless device's coverage area where they do not receive multicast packets and lose communication with the wireless device even though they are still associated to it.

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

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

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio { 0 }**	Enter interface configuration mode for the 2.4-GHz 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 the wireless devices are connected. See the "Configuring Protected Ports" section on page 2-25 for instructions on setting up protected ports.

To enable and disable PSPF using CLI commands on the wireless device, 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/bcfpart1/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** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**bridge-group** *group* **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 the wireless devices 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** *interface-id*	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** *interface-id* **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, see the "Configuring Port-Based Traffic Control" chapter in the *Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(12c)EA1* at:
http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_book09186a008011591c.html

Configuring Beacon Period and DTIM

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

For example, if the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the wireless device sends a beacon containing a DTIM every 200 kilo-microseconds. One kilo-microsecond equals 1,024 microseconds.

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

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

Configuring RTS Threshold and Retries

The RTS threshold determines the packet size at which the wireless device 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 wireless device, or in areas where the clients are far apart and can detect only the wireless device and not each other. You can enter a setting ranging from 0 to 2347 bytes.

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 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** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**rts threshold** *value*	Set the RTS threshold. Enter an RTS threshold from 0 to 2347.

	Command	Purpose
Step 4	**rts retries** *value*	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 Maximum Data Retries

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

The default setting is 15. 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** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**packet retries** *value*	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 Fragmentation Threshold

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

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**fragment-threshold** *value*	Set the fragmentation threshold. Enter a setting from 256 to 2346 bytes for the 2.4-GHz radio. Enter a setting from 256 to 2346 bytes for the 5-GHz 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 command to reset the setting to defaults.

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.

	Command	Purpose
Step 1	**router(config-if)# slot-time-short**	In radio interface mode, enter this command to enable short slot time.
Step 2	**no slot-time-short**	(optional) Enter **no slot-time-short** 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, 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.