



Configuring Radio Settings

This chapter describes how to configure radio settings for the wireless device.

Enabling the Radio Interface

The wireless device radios are disabled by default.


Note

Beginning with Cisco IOS Release 12.3(8)JA there is no SSID. You must create an SSID before you can enable the radio interface.

Beginning in privileged EXEC mode, follow these steps to enable the access point radio:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot11 ssid <i>ssid</i>	Enter the SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.
Step 3	interface dot11radio {0 1slot/port}	Enter interface configuration mode for the radio interface. The 2.4-GHz and the 802.11n 2.4-GHz radio is radio 0 The 5-GHz and the 802.11n 5-GHz radio is radio 1.
Step 4	ssid <i>ssid</i>	Assign the SSID you created in Step 2 to the appropriate radio interface.
Step 5	no shutdown	Enable the radio port.
Step 6	end	Return to privileged EXEC mode.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

Configuring the Role in Radio Network

Table 6-1 shows the role in the radio network for each device.

Table 6-1 Device Role in Radio Network Configuration

Role in Radio Network	AP 1040	AP 1140	AP 1260	AP 1530	AP 1550	AP 1600	AP 1700	AP 2600	AP 3500	AP 3600	AP 3700	AP 700	AP 2700
Access point	Yes	Yes	Yes										
Access point (fallback to radio shutdown)	Yes	Yes	Yes										
Access point (fallback to repeater)	Yes	Yes	Yes										
Repeater	Yes	Yes	Yes										
Root bridge	Yes	Yes	Yes										
Non-root bridge	Yes	Yes	Yes										
Root bridge with wireless clients	Yes	Yes	Yes										
Non-root bridge with wireless clients	Yes	Yes	Yes										
Workgroup bridge	Yes	Yes	Yes										
Universal workgroup bridge ¹	Yes	Yes	Yes										
Scanner	Yes	Yes	Yes										
Spectrum	–	–	–	–	Yes	–	Yes	Yes	Yes	Yes	Yes	–	Yes
Install [automatic non-root root]	–	–	–	Yes	–	–	–	–	–	–	–	–	–

1. When configuring a universal workgroup bridge using AES-CCM TKIP, the non-root device should use only TKIP or AES-CCM TKIP as ciphers in order to associate to the root device. The non-root device will not associate with the root if it is configured only AES-CCM. This configuration results in a mismatch in the multicast cipher between the root and non-root devices.

You can configure the role of an access point or bridge in a radio network. 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. There are two possible fallback roles:

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

**Note**

When configuring a universal workgroup bridge using AES-CCM TKIP, the non-root device should use only TKIP or AES-CCM TKIP as ciphers in order to associate to the root device. The non-root device will not associate with the root if it is configured only AES-CCM. This configuration results in a mismatch in the multicast cipher between the root and non-root devices.

Beginning in privileged EXEC mode, follow these steps to set the wireless device 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: 2.4-GHz radio and the 802.11n 2.4-GHz radio is interface 0. 5-GHz radio and the 802.11n 5-GHz radio is interface 1.

	Command	Purpose
Step 3	<pre>station-role non-root {bridge wireless-clients} repeater root {access-point ap-only bridge [wireless-clients] fallback [repeater shutdown]} scanner workgroup-bridge {multicast mode <client infrastructure> universal <Ethernet client MAC address>}</pre>	<p>Set the wireless device role.</p> <ul style="list-style-type: none"> Set the role to non-root bridge with or without wireless clients, repeater access point, root access point or bridge, scanner, or workgroup bridge. When in bridge mode, they are interoperable with outdoor access point/bridge only on supported bridge features. The bridge mode radio supports point-to-point and point-to-multipoint configuration. An outdoor access point/bridge operating as a non-root bridge can associate with another non-root bridge as long as the station role for the non-root bridge is set to non-root wireless clients. 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. A workgroup bridge can have a maximum of 254 clients, presuming that no other wireless clients are associated to the root bridge or access point. A universal workgroup bridge configures the access point in workgroup bridge mode and able to interoperate with non-Cisco access points. You must enter the Ethernet client MAC address. The workgroup bridge associates with the configured MAC address only if it is present in the bridge table and it should not be a static entry. If validation fails, the workgroup bridge associates with its BVI MAC address. Also, the universal workgroup bridge role supports only one wired client. Spanning Tree Protocol (STP) is configurable on access points in bridge modes. (Optional) Select the root access point fallback role. If the wireless device 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	<pre>end</pre>	Return to privileged EXEC mode.
Step 5	<pre>copy running-config startup-config</pre>	(Optional) Save your entries in the configuration file.

**Note**

When you enable the role in the radio network as a non root bridge or a workgroup bridge and enable the interface using the **no shut** command, the physical status and the software status of the interface will be up 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 of the device comes up only when the device on the other end is configured and up.

Universal Workgroup Bridge Mode

When configuring the universal workgroup bridge role, you must include the client MAC address. The workgroup bridge will associate with this MAC address only if it is present in the bridge table and is not a static entry. If validation fails, the workgroup bridge associates with its BVI MAC address. In universal workgroup bridge mode, the workgroup bridge uses the Ethernet client MAC address to associate with Cisco or non-Cisco root devices. The universal workgroup bridge is transparent and is not managed.

**Note**

The universal workgroup bridge role supports only one wired client.

You can enable a recovery mechanism and make the workgroup bridge manageable again by disabling the Ethernet client, causing the universal workgroup bridge to associate with an access point using its own BVI address.

The roaming keyword has been added to the interface command **world-mode dot11d country-code country** [**indoor** | **outdoor** | **both**] to support the “airline flying between different countries” scenario. The keyword causes the workgroup bridge to do passive scanning once it is deauthenticated from a root access point. See the “[Enabling and Disabling World Mode](#)” section on page 6-26 for more information on this command.

Point-to-point and Multi Point bridging support for 802.11n platforms

The point-to-point and point-to-multipoint bridging is supported on all 802.11n access points. The 5 GHz bands support 20- and 40-MHz and the 2.4-GHz bands support 20 MHz.

The following are supported on all 802.11n access points:

- MIMO, short-range bridging (on campus or inter-building bridge deployments), with dipole and MIMO antennas (line of sight and short range) under 1 Km.
- 20-MHz and 40-MHz 802.11n support.
- Workgroup bridge (WGB) short-range support.
- SISO (single-in, single-out), MCS 0-7 and legacy bridge rates (802.11 a/b/g and 802.11n) using one outdoor antenna.

**Note**

The aforementioned support is only for short range links and is not a replacement for the AP 1400 or other Bridge products.

The following are not supported by AP models with internal antennas, in their bridging modes:

- The **distance** command. The **distance** command is supported only on access points that are approved for outdoor use.
- Outdoor MIMO bridging using external antennas.

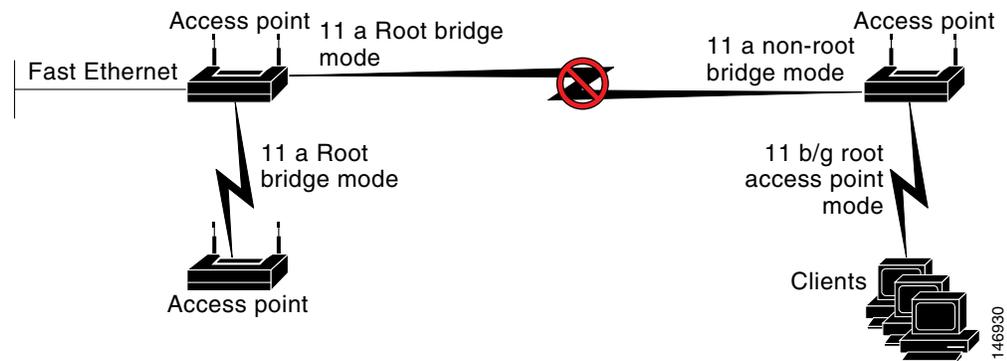
**Note**

In point-to-multipoint bridging, WGB is not recommended with the root bridge. WGB should be associated to the root AP in point-to-multipoint bridging setup.

Configuring Dual-Radio Fallback

The dual-radio fallback feature allows you to configure access points so that if the non-root bridge link connecting the access point to the network infrastructure goes down, the root access point link through which a client connects to the access point shut down. Shutting down the root access point link causes the client to roam to another access point. Without this feature, the client remains connected to the access point, but will not be able to send or receive data from the network.

Figure 6-1 Dual-Radio Fallback



Note

This feature is supported by all dual-radio access points.
This feature does not affect the fallback feature for single-radio access points.

You can configure dual-radio fallback in three ways:

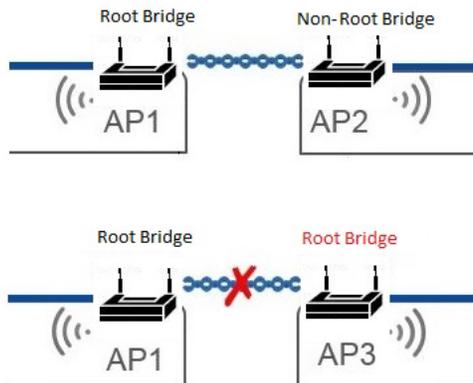
- Radio tracking
- Fast Ethernet tracking
- MAC-address tracking

Configuring Wireless Bridge Auto Negotiation

The autonomous access point can be configured as a root bridge or a non-root bridge. A wireless link can be created between the root and non-root bridges.

Figure 2 shows the connection failure caused by changes of access points with different roles. At first, AP1 is root bridge and AP2 is non-root bridge. The connection is established between AP1 and AP2. Then AP2 is removed and replaced by AP3. If AP3 has the same role of root bridge as AP1, the connection between AP1 and AP3 cannot be established until either AP1 or AP3 change to non-root bridge manually.

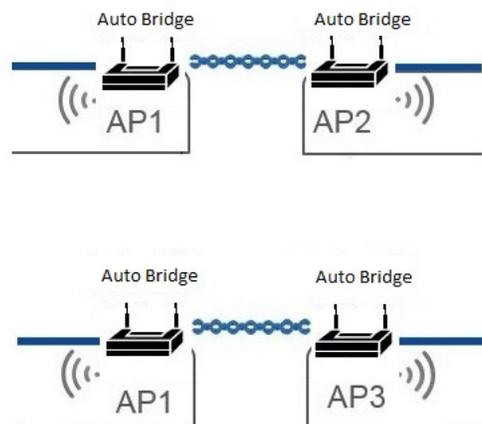
Figure 2 Changes in Train Composition Breaking Wireless Bridge Link



Configuring the access points to auto bridge mode can make this manual adjustment automatically.

The access points in auto bridge mode can detect the potential candidate for association when two access points are coming close enough to each other. The role negotiation will happen when the received RSSI is higher than a configured RSSI threshold. The access point with a lower MAC address will become the root bridge. The other will be non-root bridge. After the connection is established successfully, if the received RSSI is continuously lower than the configure threshold for 10 seconds, the access points will disassociate from each other and the access point role will be changed back to the initial auto bridge status.

Figure 3 Wireless Bridge Auto Negotiation



Even if there are more than two access points qualified for the association criteria, only one automatic bridge connection can be established. If this connection is not the correct one, when the unwanted access point moves away, the other access point can make the correct connection. In deployment, the RSSI threshold must be adjusted accordingly to avoid such situation.

For a dual radio access point, the 5 GHz radio interface can be used for wireless bridge connection, and the 2.4 GHz radio interface can be used for on-board Wi-Fi service and to accept wireless client association.

When configured with auto bridge mode, AP will be in one of the following status:

- `AUTO_ROOT_INIT`—AP works in root bridge mode and uses beacon to find potential peer AP for association.

- **AUTO_ROOT_WORKING**—AP works in configured or DFS selected channel as a root bridge.
- **AUTO_NON_ROOT**—AP works in non-root bridge mode.

When two auto bridge APs receive the beacon from each other, they will change the roles respectively. The AP with lower MAC address will change to **AUTO_ROOT_WORKING** state. Meanwhile its serving channel will be set to the configured one. The AP with higher MAC address will change its role to **AUTO_NON_ROOT**.

Failure of establishing wireless bridge link or lost of wireless association will roll back the AP to **AUTO_ROOT_INIT** role and restart discovery after time out.

A root bridge only allows a non-root bridge to associate using the infrastructure SSID. Non-root bridges use this SSID to associate with root devices. The auto bridge SSID should be configured with the **infrastructure-ssid** command for the connection to be successfully established.

**Note**

The auto bridge access point can only associate to another auto bridge access point. It cannot associate to an access point of other mode, and will not accept other client associations.

**Note**

The wireless bridge auto-negotiation feature is supported only on the IW3700 series.

Recommended Antennas

A directional and low gain antenna is recommended for this wireless bridge auto negotiation connection. A directional antenna directs signal at a specific narrow angle, which can be oriented at the target access point and reduce the risk of incorrect bridge connections.

Configuring Wireless Bridge Auto Negotiation

Beginning in privileged EXEC mode, follow these steps to configure the radio interface to work in auto bridge mode and configure the RSSI 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.
Step 3	station-role auto-bridge	Configure the radio interface to auto bridge role.
Step 4	auto-bridge rx-sensitivity <dbm>	Configure RSSI threshold for the radio interface. This command is available only if the access point is in auto bridge mode. The default value of RSSI threshold is -40 dBm.
Step 5	end	Return to privileged EXEC mode.

Configuration Example

```
dot11 ssid auto-bridge
  vlan 910
  authentication open
  authentication key-management wpa version 2
  infrastructure-ssid
  wpa-psk ascii 7 00554155500E5D5157
```

```

!
dot11 ssid passenger-wifi
    vlan 911
    authentication open
    authentication key-management wpa version 2
    wpa-psk ascii 7 00554155500E5D5157
!
interface Dot11Radio0
    encryption mode ciphers aes-ccm
    encryption vlan 911 mode ciphers aes-ccm
    ssid passenger-wifi
    station-role root
!
interface Dot11Radio0.910
    encapsulation dot1Q 910 native
    bridge-group 1
!
interface Dot11Radio0.911
    encapsulation dot1Q 911
    bridge-group 2
!
interface Dot11Radio1
    encryption mode ciphers aes-ccm
    ssid auto-bridge
    channel width 80
    station-role auto-bridge
    auto-bridge rx-sensitivity 40
!
interface Dot11Radio1.910
    encapsulation dot1Q 910 native
    bridge-group 1
!
interface Dot11Radio1.911
    encapsulation dot1Q 911
    bridge-group 2
!
interface GigabitEthernet0
    no ip address
    duplex auto
    speed auto
!
interface GigabitEthernet0.910
    encapsulation dot1Q 910 native
    bridge-group 1
!
interface GigabitEthernet0.911
    encapsulation dot1Q 911
    bridge-group 2

```

(Optional) Configuring Channel

The existing channel configuration command is also available for the auto bridge mode. The serving channel and channel width can be configure using following command:

```

(config-if)# channel ?
  <36-5825>  One of: 36 40 44 48 149 153 157 161 165 5180 5200 5220 5240 5745
              5765 5785 5805 5825
  dfs       Use Dynamic Frequency Selection
  width     Bandwidth

```

Verifying the Auto Bridge Status

Use the following command to display the current auto bridge role and status:

```
# show controllers d1 frequency
```

```
DFS Blocked Frequencies: none
Beacon Flags: 0, Interface Flags 20105, Interface Events 0, Mode 4004; Beacons are
disabled; Probes are disabled
mode AUTO_NON_ROOT, status: access point (with client) is now working stably
```

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 on radio 1:

```
# station-role root access-point fallback track d0 shutdown
```
- To track radio 1, enter the following command on radio 0:

```
# station-role root access-point fallback track d1 shutdown
```

Fast Ethernet Tracking

You can configure the access point for fallback when its Ethernet port is disabled or disconnected from the wired LAN. You configure the access point for fast Ethernet tracking as described in the [“Configuring the Role in Radio Network” section on page 6-3](#).



Note

Fast Ethernet tracking does not support the Repeater mode.

- To configure non-802.11n access points for Fast Ethernet tracking, in the radio interfaces configuration mode enter the following command:

```
# station-role root access-point fallback track fa 0
```
- To configure 802.11n access points for Gigabit Ethernet tracking, in the radio interfaces configuration mode enter the following command:

```
# station-role root fallback shutdown
```

MAC-Address Tracking

You can configure the radio whose role is root access point to go up or down by tracking a non-root bridge or workgroup bridge, 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 non-root bridge or workgroup bridge, having a MAC address 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
```

Limiting Clients per Radio

You can set the number of clients allowed for association with an interface, using the command **max-client** *1-255*, under the dot11 radio interface configuration. This setting is disabled by default. The minimum number of clients allowed is 1 and the maximum is 255.

```
ap(config-if)# max-client 1-255
```

For setting this via the GUI:

-
- Step 1** Go to **Network > Network Interfaces**.
 - Step 2** On the side menu, click Dot11 Radio 2.4 GHz or Dot11 Radio 5 GHz depending on which radio interface you want to limit the clients.
 - Step 3** On the radio interface's settings page, you can either enable or disable the **Max-Client** option.
 - Step 4** If you enable the Max-Client option, then in the text box provided alongside the Max-Client option, specify the number of clients allowed for association with the interface.
 - Step 5** Click **Apply**.
-

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 attempts to transmit at the highest data rate set on the CLI or GUI interfaces. If there are obstacles or interference, the wireless device steps down to the next lower 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. 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**.

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**. 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 is not able to connect to the access point while other clients can, one reason may be because the client is not within the coverage area of the access point. In such a case using the range option will help in extending 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 will renegotiate down in order to maintain the link (but at a lower data rate). Contrast that against a link configured for a higher throughput that will simply drop when the signal degrades enough to no longer sustain a configured high data rate, or roam to another access point with sufficient coverage, if one is available. The balance between the two (throughput vs. range) is one of those design decisions that has to be made based on resources available to the wireless project, type of traffic the users will be passing, 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 data rates to **basic** (i.e. 12 rates for 2.4 Ghz and 8 rates for 5 GHz).

**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 Mbps are set to required (**basic**) and that all other data rates are set to **enable**. The 802.11b adapters do not recognize the 802.11g rates and do not operate if data rates higher than 11Mbps are set to require on the connecting access point.

Access Points Send Multicast and Management Frames at Highest Basic Rate

Access points running recent Cisco IOS versions are transmitting multicast and management frames at the highest configured basic rate, and is a situation that could causes reliability problems.

Access points running LWAPP or autonomous IOS should transmit multicast and management frames at the lowest configured basic rate. This is necessary in order to provide for good coverage at the cell's edge, especially for unacknowledged multicast transmissions where multicast wireless transmissions may fail to be received.

Since multicast frames are not retransmitted at the MAC layer, stations at the edge of the cell may fail to receive them successfully. If reliable reception is a goal, then multicasts should be transmitted at a low data rate. If support for high data rate multicasts is required, then it may be useful to shrink the cell size and to disable all lower data rates.

Depending on your specific requirements, you can take the following action:

- If you need to transmit the multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, one that is low enough to reach the edges of the wireless cells.
- If you need to transmit the multicast data at a certain data rate in order to achieve a certain throughput, then configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of non-multicast clients.

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 1slot/port}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and 2.4-GHz N radio is radio 0, and the 5-GHz radio and 5-GHz N radios radio 1.

	Command	Purpose
<p>Step 3</p> <p>speed</p> <p>802.11g, 2.4-GHz radio:</p> <pre>{[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 }</pre> <p>802.11a 5-GHz radio:</p> <pre>{[6.0] [9.0] [12.0] [18.0] [24.0] [36.0] [48.0] [54.0] [basic-6.0] [basic-9.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-54.0] range throughput ofdm-throughput default }</pre> <p>802.11n 2.4-GHz radio:</p> <pre>{[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 }</pre> <p>802.11n 5-GHz radio:</p> <pre>{[12.0] [18.0] [24.0] [36.0] [48.0] [54.0] [6.0] [9.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-54.0] [basic-6.0] [basic-9.0] [default] [m0-7] [m0.] [m1.] [m10.] [m11.] [m12.] [m13.] [m14.] [m15.] [m2.] [m3.] [m4.] [m5.] [m6.] [m7.] [m8-15] [m8.] [m9.] range throughput }</pre>	<p>Set each data rate to basic or enabled, or enter range to optimize range or throughput to optimize throughput.</p> <ul style="list-style-type: none"> (Optional) 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. <p>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 802.11g radio.</p> <p>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.</p> <p>(Optional) Alternatively, 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 the other rates to enabled. When you enter throughput, the wireless device sets all data rates to basic.</p> <p>(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.</p> <ul style="list-style-type: none"> (Optional) Enter default to set the data rates to factory default settings (not supported on 802.11b radios). <p>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 802.11g radio.</p> <p>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.</p>	

	Command	Purpose
	speed (continued)	On the 802.11n 2.4-GHz radio, the default option sets rates 1.0, 2.0, 5.5, and 11.0 to enabled. On the 802.11n 5-GHz radio, the default option sets rates to 6.0, 12.0, and 24.0 to enabled. The default MCS rate setting for both 802.11n radios is 0–15.
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:

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

Configuring MCS Rates

Modulation Coding Scheme (MCS) is a specification of PHY parameters consisting of modulation order (BPSK, QPSK, 16-QAM, 64-QAM) and FEC code rate (1/2, 2/3, 3/4, 5/6). MCS is used in 802.11n radios, which define 32 symmetrical settings (8 per spatial stream):

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

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*. 802.11 a, b, and g radios use 20-MHz channel widths.



Tip

For the latest information on the Data Rates based on MCS Index, Guard Interval (GI), and channel width, for you access point, refer to its *Cisco Aironet (AP series name) Series Access Points Data Sheet* on the Cisco.com site.

MCS rates are configured using the **speed** command. The following example shows a **speed** setting for an 802.11n 5-GHz radio:

```
interface Dot11Radio0
  no ip address
  no ip route-cache
  !
  ssid 1260test
  !
  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.
```

Enabling 11ac MCS rates

MCS rates are configured using the **speed** command.

To enable 11ac rates, it is mandatory to have at least one basic rate and one 11n rate enabled.

The following example shows a **speed** setting for an 802.11ac 5-GHz radio:

```
interface Dot11Radio1
!
!
ssid 11ac
!
speed 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7. m8. m9. m10.
m11. m12. m13. m14. m15. m16. m17. m18. m19. m20. m21. m22. m23. a1ss9 a2ss9 a3ss9
Channel width 80
```

Configuring unicast-mcs-only

If you want to configure the autonomous AP to transmit data only at MCS rate, use the command **speed unicast-mcs-only**.



Note

This command applies to both 2.4G and 5G radio interface, but only available for WGB mode of the Cisco IW3702 access point.

For example, assume the configured rate set for WGB radio is basic-12.0 m0. m1. m2. m3. m4.

By default, **speed unicast-mcs-only** is disabled. All the configured rate (basic-12.0 m0. m1. m2. m3. m4.) is available for data transmit.

When **speed unicast-mcs-only** is enabled, unicast data transmitting rate will be limited to the MCS range of m0. m1. m2. m3. m4. Other data, such as management frames broadcast or multicast data, will be transmitted in mandatory rate (basic rates).

The following example shows the configuration of **speed unicast-mcs-only**:

```
interface Dot11Radio1
no ip address
!
encryption mode ciphers aes-ccm
!
ssid 11i
!
antenna gain 0
antenna a-antenna
peakdetect
ampdu transmit priority 1
ampdu transmit priority 3
ampdu transmit priority 6
ampdu transmit priority 7
amsdu transmit priority 6
amsdu transmit priority 7
speed unicast-mcs-only
speed basic-12.0 m0. m1. m2. m3. m4.
packet retries 32 drop-packet
station-role workgroup-bridge
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 6-2 shows the relationship between mW and dBm.

Table 6-2 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 1slot/port}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The 2.4-GHz 802.11n radio is 0, and the 5-GHz 802.11n radio is 1
Step 3	power local These options are available for the 802.11a, 5-GHz radio (in dBm), and for the 2.4-GHz 802.11n radio (in dBm): {22 19 16 13 10 7 4}	Set the transmit power for the 802.11b, 2.4-GHz radio or the 5-GHz radio to one of the power levels allowed in your regulatory domain. Note See the hardware installation guide for your access point to determine the power settings for your regulatory domain.

	Command	Purpose
Step 4	<p>power local</p> <p>These options are available for the 802.11g, 2.4-GHz radio:</p> <p>power local cck settings: { -1 2 5 8 11 14 17 20 maximum }</p> <p>power local ofdm settings: { -1 2 5 8 11 14 17 maximum }</p> <p>Note These options are not available on 802.11n APs.</p>	<p>Set the transmit power for the 802.11g, 2.4-GHz radio to one of the power levels allowed in your regulatory domain. Settings are in dBm.</p> <p>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.</p> <p>Note See the hardware installation guide for your access point to determine the power settings for your regulatory domain.</p> <p>Note The 802.11g radio maximum transmission power level depends the AP model. See the AP data sheet for the power levels.</p>
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 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 1slot/port}	<p>Enter interface configuration mode for the radio interface.</p> <p>The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.</p> <p>The 2.4-GHz 802.11n radio is 0, and the 5-GHz 802.11n radio is 1.</p>

	Command	Purpose
Step 3	<p>power client</p> <p>These options are available for both 802.11n 2.4-GHz and 5-GHz clients (in dBm):</p> <p>{-127 to 127 local maximum}</p>	<p>Set the power level allowed on client devices that associate to the wireless device. You can:</p> <ul style="list-style-type: none"> • Set any power level value in dBm from -127 to 127 • Set the power level to local, to set the client power level to that of the access point. • Set the power level to maximum, to set the client power to the allowed maximum. <p>Note The settings allowed in your regulatory domain might differ from the settings listed here.</p>
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

**Note**

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

Configuring Radio Channel Settings

The default channel setting for the 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.

**Note**

In places where RF interference might be causing clients to occasionally get disconnected from the wireless network, setting the wireless interface to run on a different channel, such as channel 1 (2412), might avoid the interference.

Each 2.4-GHz channel covers 22 MHz. The channels 1, 6, and 11 do 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 9 channels from 5180 to 55825 MHz on 802.11n APs, and on 8 channels from 5180 to 5805 on 1140 series APs. 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.

Because they change frequently, channel settings are not included in this document. For up-to-date information on channel settings for your access point or bridge, see the *Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges*. This document is available on cisco.com at the following URL:

http://cisco.com/en/US/products/ps6521/tsd_products_support_install_and_upgrade.html

Channel Widths for 802.11n

802.11n allows both 20-MHz and 40-MHz channel widths consisting of 2 contiguous non-overlapping channels (for example, 5-GHz channels 36 and 40). 802.11n radios operate in the same band. However the channel widths can be independently configured.

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

A 40-MHz channel is specified as a channel and -1 as extension. So here, the control channel is channel 40-MHz and the extension channel is 36-MHz below it.

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio {0 1slot/port}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 802.11n 2.4-GHz is radio 0. The 5-GHz radio and the 802.11n 5-GHz is radio 1.
Step 3	channel {frequency least-congested width [20 40-above 40-below] dfs}	Set the default channel for the wireless device radio. To search for the least-congested channel on startup, enter least-congested . Use the width option to specify a bandwidth to use. This option is available on all 802.11n APs, but only for the d1 (5 GHz) radio. It has three settings: 20, 40-above, and 40-below. Choosing 20 sets the channel width to 20 MHz. Choosing 40-above sets the channel width to 40 MHz with the extension channel above the control channel. Choosing 40-below sets the channel width to 40 MHz with the extension channel below the control channel. Note The channel command is disabled for 5-GHz radios that comply with European Union regulations on dynamic frequency selection (DFS). See the “ Setting the 802.11n Guard Interval ” section on page 6-26 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.

Dynamic Frequency Selection

Access points with 5-GHz radios configured at the factory for use in the United States, Europe, Singapore, Korea, Japan, Israel, and Taiwan now comply with regulations that require radio devices to use Dynamic Frequency Selection (DFS) to detect radar signals and avoid interfering with them. When an access point detects a radar on a certain channel, it avoids using that channel for 30 minutes. 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 6-3](#), the access point automatically uses DFS to set the operating frequency. 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.
- If participating in WDS, sends a DFS notification to the active WDS device that it is leaving the frequency.
- Randomly selects a different 5-GHz channel.
- If the channel selected is one of the channels in [Table 6-3](#), 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.
- If participating in WDS, sends a DFS notification of its new operating frequency to the active WDS device.



Note

You cannot manually select a channel for DFS-enabled 5-GHz radios in some regions, depending on the regulatory requirements. The access points randomly selects a channel in that case.

The full list of channels that require DFS is shown in [Table 6-3](#).

Table 6-3 DFS Channel List

Channel	Frequency	Channel	Frequency	Channel	Frequency
52	5260 MHz	104	5500 MHz	124	5620 MHz
56	5280 MHz	108	5520 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

For autonomous operation, DFS requires random channel selection among the channels listed in [Table 6-3](#). The channels not listed in [Table 6-3](#) do not require random selection and may be manually configured.

Channels requiring Dynamic Frequency Selection (DFS) may be manually selected from the 5 GHz radio configuration menu. To know the DFS channels, use the **show controllers d1** command.

The GUI/CLI used to manually configure non-DFS channels can also be used to select DFS channels as well. The default channel selection is "DFS", which randomly selects a channel.

If radar is detected on a manually configured DFS channel, the channel will be changed automatically and will not return to the configured channel.

Prior to transmitting on any channels listed in [Table 6-3](#), the access point radio performs a Channel Availability Check (CAC). The CAC is a 60 second scan for the presence of radar signals on the channel. The following sample messages are displayed on the access point console showing the beginning and end of the CAC scan:

```
*Mar 6 07:37:30.423: %DOT11-6-DFS_SCAN_START: DFS: Scanning frequency 5500 MHz for 60 seconds
```

```
*Mar 6 07:37:30.385: %DOT11-6-DFS_SCAN_COMPLETE: DFS scan complete on frequency 5500 MHz
```

When operating on any of the DFS channels listed in [Table 6-3](#), having already performed the CAC, the access point constantly monitors the channel for radar. If radar is detected, the access point stops forwarding data packets within 200 ms and broadcasts five beacons that include an 802.11h channel switch announcement, indicating the channel number that the access point begins using. The following example message displays on the access point console when radar is detected:

```
*Mar 6 12:35:09.750: %DOT11-6-DFS_TRIGGERED: DFS: triggered on frequency 5500 MHz
```

When radar is detected on a channel, that channel may not be used for 30 minutes. The access point maintains a flag in non-volatile storage for each channel that it detects radar on in the last 30 minutes. After 30 minutes, the flag is cleared for the corresponding channel. If the access point is rebooted before a flag is cleared, the non-occupancy time is reset to 30 minutes when the channel initializes.

**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.

Radar Detection on a DFS Channel

If your AP is installed near a radar station, it may detect radar activity on multiple channels. By using the **peakdetect** command on interface dot11radio1, you can ensure that the AP will detect radar signals and avoid interfering with them using Dynamic Frequency Selection (DFS). By default this command is enabled.

However, in cases where you suspect that the APs are getting false DFS triggers due to in-band/off-channel weather radar signals that cannot be resolved using physical RF signal filters, you can set the AP to not detect radar signals. If you do not want the AP to detect radar signals, use the **no peakdetect** command on interface dot11radio1.

When an access point detects a radar on a DFS channel, the access point creates a file in its flash memory. The file is based on the 802.11a radio serial number and contains the channel numbers on which the radar is detected. This is an expected behavior and you should not remove this file.

CLI Commands

The following sections describe CLI commands that apply to DFS.

Confirming that DFS is Enabled

Use the **show controllers dot11radio1** command to confirm that DFS is enabled. The command also includes indications that uniform spreading is required and channels that are in the non-occupancy period due to radar detection.

This example shows a line from the output for the show controller command for a channel on which DFS is enabled. The indications listed in the previous paragraph are shown in **bold**:

```
ap#sh controllers dot11Radio 1
!
interface Dot11Radio1
Radio ElliotNess 5, Base Address f4ea.6710.6590, BBlock version 0.00, Software version
4.10.1
Serial number: FOC16145K24
Unused dynamic SDRAM memory: 0x00007CB4 (31 KB)
Unused dynamic SDRAM memory: 0x0008E490 (569 KB)
Spectrum FW version: 1.14.2
Number of supported simultaneous BSSID on Dot11Radio1: 16
Carrier Set: Americas (OFDM) (US) (-A)
Uniform Spreading Required: Yes
Configured Frequency: 0 MHz Channel 0
Allowed Frequencies: * Dynamic Frequency Selection (DFS) only
    5180( 36)  5200( 40)  5220( 44)  5240( 48)  *5260( 52) *5280( 56) *5300( 60)
*5320( 64) *5500(100) *5520(104)
    *5540(108) *5560(112) *5580(116) *5660(132) *5680(136) *5700(140)  5745(149)
5765(153)  5785(157)  5805(161)
    5825(165)
Listen Frequencies:
    5180( 36)  5200( 40)  5220( 44)  5240( 48)  5260( 52)  5280( 56)  5300( 60)
5320( 64)  5500(100)  5520(104)
    5540(108)  5560(112)  5580(116)  5600(120)  5620(124)  5640(128)  5660(132)
5680(136)  5700(140)  5745(149)
    5765(153)  5785(157)  5805(161)  5825(165)

DFS Blocked Frequencies: none
Beacon Flags: 0, Interface Flags 20109, Interface Events 0, Mode 9; Beacons are disabled;
Probes are disabled
Configured TxPower:                14 dBm
Allowed Power Levels:              14 11  8  5  2 dBm
Allowed Client Power Levels:       14 11  8  5  2 dBm
Antenna:                            Rx[a b c d ]
                                    Tx[a b c d ofdm all]
                                    External
                                    Gain [Allowed 12, Reported 0, Configured 0, In Use 12]

(dBi x 2)
```

Configuring a Channel

Use the **channel** command to configure a channel. The command for the interface is modified to only allow you to select a specific channel number and to enable DFS.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio1 dfs	Enter the configuration interface for the 802.11a radio
Step 3	channel {number dfs band <1 - 4>}	For <i>number</i> , enter a channel frequency from 36 to 5825. Enter dfs and one of the following frequency bands to use dynamic frequency selection on the selected channel: 1—5.150 to 5.250 GHz 2—5.250 to 5.350 GHz 3—5.470 to 5.725 GHz 4—5.725 to 5.825 GHz If you attempt to configure a channel that may only be selected by dfs, the following message appears: This channel number/frequency can only be used by Dynamic Frequency Selection (DFS) Note The channel dfs command is not supported in -P and -Q regulatory domains.
Step 4	end	Return to the privileged EXEC mode.
Step 5	show running-config	Verify your entries
Step 6	copy running-config startup-config	(Optional) Save your entries to the configuration file.

The following example configures the 5 GHz radio to use DFS:

```
ap# configure terminal
ap(config)# interface dot11radio1
ap(config-if)# channel dfs
ap(config-if)# end
```

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. This group of frequencies is also known as UNII-2 extended.

- **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:

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

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

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

This example shows how to unblock all frequencies for DFS:

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

Setting the 802.11n Guard Interval

The 802.11n guard interval is the period in nanoseconds between packets. Two settings are available: short (400ns) and long (800ns).

Beginning in privileged EXEC mode, follow these steps to set the 802.11n guard interval.

	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 802.11n 2.4-GHz radio is radio 0 The 802.11n 5-GHz radio is radio 1.
Step 3	guard-interval {any long}	Enter a guard interval. <ul style="list-style-type: none"> • any—allows the AP to use 400 ns with clients supporting short GIs, and 800 ns with clients not supporting short GIs, i.e. either the short (400ns) or long (800ns) guard interval. • long—allows only the long (800ns) guard interval.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Enabling and Disabling World Mode

You can configure the wireless device to support 802.11d world mode, Cisco legacy world mode, or world mode roaming. When you enable world mode, the AP adds channel carrier set information to its beacon. Client devices with world mode enabled receive the carrier set information and adjust their settings automatically. For example, a client device used primarily in Japan could rely on world mode to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

World mode is disabled by default.

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio {0slot/port 1}</code>	Enter interface configuration mode for the radio interface.
Step 3	<code>world-mode</code> <code>dot11d country_code code</code> <code>{ both indoor outdoor }</code> <code>world-mode roaming</code> <code> legacy</code>	<p>Enable world mode.</p> <ul style="list-style-type: none"> Enter the dot11d option to enable 802.11d world mode. <ul style="list-style-type: none"> When you enter the dot11d option, you must enter a two-character ISO country code (for example, the ISO country code for the United States is US). You can find a list of ISO country codes at the ISO website. After the country code, you must enter indoor, outdoor, or both to indicate the placement of the wireless device. Enter the legacy option to enable Cisco legacy world mode. Enter the world-mode roaming to place the access point in a continuous world mode configuration. <p>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.</p>
Step 4	<code>end</code>	Return to privileged EXEC mode.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

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

Disabling and Enabling Short Radio Preambles

The radio preamble is a section of data at the head of a frame that helps the APs and clients to synchronize their communication. You can set the radio preamble to long or short:

- Short—A short preamble improves throughput performance. Cisco Aironet Wireless LAN Client Adapters support short preambles. Any 802.11b or 802.11g certified device supports short preambles. However, some client devices still require long preambles, even when they are 802.11b/g certified.
- Long—Long preambles are used by legacy 802.11 only devices, and some 802.11b/g devices that expect long preambles for optimal operations. 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 { 0slot/port }	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:

- **Gain**—Sets the resultant antenna gain in 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. If the device has three removable antennas, you can use this setting to have all of them operate in diversity mode.
- **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.
- **Middle**—If the wireless device has removable antennas and you install a high-gain antenna on the wireless device middle connector, you should use this setting for receiving only. The antennas available for transmitting in a three-antenna configuration are the right and left antennas.
- **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.
This does not apply for dual antenna APs such as the 1600, 2600, and 3600 series. Please check the respective hardware guides for further information.

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 1slot/port }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The 802.11n 2.4-GHz radio is radio 0 The 802.11n 5-GHz radio is radio 1.

	Command	Purpose
Step 3	<code>antenna again dB</code>	Specifies the resultant gain of the antenna attached to the device. Enter a value from –128 to 128 dB. Note This setting does not affect the behavior of the wireless device; it only informs the management platform on your network of the device antenna gain.
Step 4	<code>antenna receive</code> { <code>diversity</code> <code>left</code> <code>middle</code> <code>right</code> } On the 2600 and the 3600 series, this command is: <code>antenna receive</code> { <code>a-antenna</code> <code>ab-antenna</code> <code>abc-antenna</code> <code>abcd-antenna</code> }	Set the receive antenna to diversity, left, middle, right, or all. 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 . On the 2600 and the 3600 series APs: <ul style="list-style-type: none"> • <code>a-antenna</code>—to use antenna A • <code>ab-antenna</code>—to use antennas A and B • <code>abc-antenna</code>—to use antennas A, B, and C • <code>abcd-antenna</code>—to use antennas A, B, C, and D
Step 5	<code>antenna transmit</code> { <code>diversity</code> <code>left</code> <code>right</code> } On the 2600 and the 3600 series, this command is: <code>antenna transmit</code> { <code>a-antenna</code> <code>ab-antenna</code> <code>abc-antenna</code> <code>abcd-antenna</code> }	Set the transmit antenna to diversity, left, or right. 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 . On the 2600 and the 3600 series APs: <ul style="list-style-type: none"> • <code>a-antenna</code>—to use antenna A • <code>ab-antenna</code>—to use antennas A and B • <code>abc-antenna</code>—to use antennas A, B, and C • <code>abcd-antenna</code>—to use antennas A, B, C, and D
Step 6	<code>end</code>	Return to privileged EXEC mode.
Step 7	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Enabling and Disabling Gratuitous Probe Response

Gratuitous Probe Response (GPR) aids in conserving battery power in dual mode phones that support cellular and WLAN modes of operation. GPR is available on 5-GHz radios and is disabled by default. You can configure two GPR settings:

- **Period**—This setting determines the time between GPR transmissions in Kusec (or milliseconds) intervals from 10 to 255 (similar to the beacon period)
- **Speed**—The speed is the data rate used to transmit the GPR

Selecting a longer period reduces the amount of RF bandwidth consumed by the GPR with the possibility of shorter battery life. Selecting higher transmission speeds also reduces the amount of bandwidth consumed but at the expense of a smaller cell size.

Beginning in privileged EXEC mode, follow these steps to enable GPR and set its parameters:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio {1}slot/port	Enter interface configuration mode for the 5-GHz radio interface.
Step 3	probe-response gratuitous {period speed}	Enable the Gratuitous Probe Response feature using default period (10 Kusec) and speed (6.0 Mbps).
Step 4	period Kusec	(Optional) Enter a value from 10 to 255. The default value is 10
Step 5	speed { [6.0] [9.0] [12.0] [18.0] [24.0] [36.0] [48.0] [54.0] }	(Optional) Sets the response speed in Mbps. The default value is 6.0.
Step 6	end	Return to privileged EXEC mode.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The optional parameters can be configured independently or combined when you do not want to use the defaults, as shown in the following examples:

```
(config-if)# probe-response gratuitous period 30
(config-if)# probe-response gratuitous speed 12.0
(config-if)# probe-response gratuitous period 30 speed 12.0
```

Use the **no** form of the command to disable the GPR feature.

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 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.
- Cisco Key Integrity Protocol (CKIP)—Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group. The standards-based algorithm, TKIP, does not require Aironet extensions to be enabled.
- Repeater mode—Aironet extensions must be enabled on repeater access points and on the root access points to which they associate.
- 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. Beginning in privileged EXEC mode, follow these steps to disable Aironet extensions:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio {0 1slot/port} }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The 802.11n 2.4-GHz radio is radio 0 The 802.11n 5-GHz radio is radio 1.
Step 3	no dot11 extension aironet	Disable Aironet 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 Aironet extensions if they are disabled.

Configuring the Ethernet Encapsulation Transformation Method

Frames contain a field that specifies the upper Layer protocol that should be used (such as IP, IPX, ARP, etc). This field is necessary at the receiver level to direct the frame properly in the receiver network stack.

There are two main techniques for protocol indication:

- **EtherType**—A 16 bit value that indicates the protocol carried in the frame. EtherType is used in Ethernet 2.0/DIX networks.
- **LLC/SNAP**—A 6 byte header that allows for an 802.2 link layer protocol indication. LLC/SNAP is used in 802.3 and 802.11 networks.

When the access point receives from the wired network frames that use EtherType information, it needs a mechanism to convert this EtherType information to SNAP/LLC information. There are two transformation methods:

- **802.1H**—This method provides good performance for Cisco Aironet wireless products.
- **RFC 1042**—Use this setting to ensure good interoperability with non-Cisco Aironet wireless equipment. RFC 1042 is used by other manufacturers of wireless equipment and is the default setting. 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 1slot/port} }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The 802.11n 2.4-GHz radio is radio 0 The 802.11n 5-GHz radio is radio 1.

	Command	Purpose
Step 3	<code>payload-encapsulation rfc1042 dot1h</code>	Set the encapsulation transformation method to RFC 1042 (<code>rfc1042</code> , the default setting) or 802.1h (<code>dot1h</code>).
Step 4	<code>end</code>	Return to privileged EXEC mode.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

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 up to 20 Cisco Aironet Workgroup Bridges that are associated to the AP. The default setting, **disabled**, reduces the reliability of multicast delivery but allows 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 and some broadcast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge.

The AP sends multicast frames to a multicast address, and then again sends the multicast frames to the workgroup bridge, encapsulated in a unicast frame, that is acknowledged by the workgroup bridge. This verification mechanism creates wireless overhead, and reduces the throughput on the access point.

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

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



Note To configure reliable multicast forwarding, this configuration should be done on the AP, and not on the workgroup bridge.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio {0 1}	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.

The workgroup bridge will start receiving the multicast frame and then the unicast copy of the same frame, which results in duplication of frames at the receiver level and is therefore inefficient.

To configure the workgroup bridge to consider only the multicast frame or the unicast copy at the workgroup bridge radio level, use the following commands:

Command	Purpose
station-role workgroup-bridge multicast mode { client infrastructure }	<p>You can set either one of the following:</p> <ul style="list-style-type: none"> Client—Client-mode accepts only 3-MAC address header multicast packets Infrastructure—Infrastructure-mode accepts only 4-MAC address header multicast packets <p>If you set reliable multicast on the AP, then you are recommended to use infrastructure at workgroup bridge level. If you do not set reliable multicast at the AP, use client at the workgroup bridge level.</p>

For example, the following command uses infrastructure at the workgroup bridge level:

```
WGB(config-if)# station-role workgroup-bridge multicast mode infrastructure
```

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 6-35 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/bcpart1/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 1slot/port}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The 802.11n 2.4-GHz radio is radio 0 The 802.11n 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 with different access points on your wireless LAN, you can set up protected ports on the switch to which the wireless devices are connected. Alternatively, you should isolate ports on the same switch that leads to APs between which you do not want communication to occur.

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

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

To disable protected port, use the **no switchport protected** interface configuration command. This command is only valid at an individual switch level. It does not isolate APs connected to different switches. You can use this command on ports to all APs on a given switch among which you do not want communication to occur. Alternatively, you can use private VLAN configuration for the AP.



Note

When using wireless domain services (WDS), make sure not to block communication between the APs and their WDS.

For detailed information on configuring private VLANs and on protected ports and port blocking, see the *Catalyst 3750 Software Configuration Guide*, at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750.html

Configuring the Beacon Period and the DTIM

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

For example, if the beacon period is set at 100, its default setting, and the DTIM is set at 2, its default setting, then the AP sends a beacon containing a DTIM every 2 beacons, or every 200 Kμsec, or every 200 ms. One Kμsec equals 1,024 microseconds.

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio {0 1slot/port}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 802.11n 2.4-GHz radio is 0. The 5-GHz radio and the 802.11n 5-GHz radio is 1.
Step 3	beacon period value	Set the beacon period in the range 20 to 4000. Enter a value in Kilomicroseconds.
Step 4	beacon dtim-period value	Set the DTIM in the range 1 to 100. 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.

Configure 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 23472347 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 2347 for all access points and bridges, and the default maximum RTS retries setting is 3264. 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 1slot/port}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.

	Command	Purpose
Step 3	rts threshold <i>value</i>	Set the RTS threshold. Enter an RTS threshold from 0 to 23472347.
Step 4	rts retries <i>value</i>	Set the maximum RTS retries. Enter a setting from 1 to 128.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

Configuring the Maximum Data Packet 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 32. Beginning in privileged EXEC mode, follow these steps to configure the maximum data retries:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio {0 1slot/port}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	packet retries <i>value</i> [drop-packet]	Set the maximum data retries. Enter a setting from 1 to 128. If the drop-packet option is used, the device stops trying to send the current packet, and moves on to try sending the next packet in the queue, without disconnecting. When the drop-packet option is not used, the wireless device determines that the link is not usable anymore, stops trying to send the current packet and terminates the connection.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

Configuring the Fragmentation Threshold

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

The default setting is 23382346 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 1slot/port}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 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.

Configuring the CCA Threshold

Clear Channel Assessment (CCA) is a mechanism for determining whether the channel is idle or not before actually transmitting. The device physically listens to the channel. If the channel power is above a predefined threshold, the channel is considered busy and the transmitting will not start.



Note

This configuration is supported only on the IW3702 platform.

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio {0 1slot/port}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	cca-threshold value	Configure the CCA threshold for the radio interface. The CCA threshold value range is from 30 to 100, which means -100dBm to -30 dBm.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring the RX-SOP Threshold

Receiver Start of Packet Detection Threshold (Rx SOP) determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. As the Wi-Fi level increases, the radio sensitivity decreases and the receiver cell size becomes smaller. Reduction of the cell size affects the distribution of clients in the network.

Rx SOP is used to address clients with weak RF links, sticky clients, and client load balancing across access points. Rx SOP helps to optimize the network performance at high-density deployments such as stadiums and auditoriums where access points need to optimize the nearest and strongest clients.



Note This configuration is supported only on the IW3702 platform.

Beginning in privileged EXEC mode, follow these steps to configure the Receiver Start of Packet Detection (RX-SOP) threshold:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio {0 1slot/port}</code>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	<code>rxsop-threshold value</code>	Configure the RX-SOP threshold for the radio interface. The RX-SOP threshold value range is from 60 to 100, which means -100dBm to -60 dBm.
Step 4	<code>end</code>	Return to privileged EXEC mode.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

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 not supported by 802.11b clients. If you enable short slot time, 802.11b clients will not be able to join or communicate with the AP radio. Short slot time is disabled by default.

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

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

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



Note

The interface must be enabled for the carrier busy test to be performed.

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

```
ap#dot11 dot11Radio 1 carrier busy
ap#show dot11 carrier busy
Frequency  Carrier Busy %
-----
5180      2
5200      0
5220      2
5240      1
5260      1
5280      0
5300      1
5320      0
5500      0
5520      0
5540      0
5560      0
5580      0
5660      0
5680      0
5700      0
5745      0
5765      0
5785      0
5805      0
5825      0
```

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 Wireless class of service 5 (Video) and wireless class of service 6 (Voice).

Follow these steps to configure VoIP packet handling on an access point:

-
- Step 1** Using a browser, log in to the access point.
 - Step 2** Click **Services** in the task menu at the top of the web-browser interface.
 - Step 3** In the left menu, 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 list and enter a value for maximum retries for packet discard in the corresponding field. Packets in other queues are dequeued, giving delay-sensitive data preferential treatment over other traffic.

The default value for maximum retries is 3 for the Low Latency setting (Figure 6-4). This value indicates how many times the access point will try to resend a lost packet before discarding it.



Note

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

Step 6 Click **Apply**.

Figure 6-4 Packet Handling Configuration

Packet Handling per User Priority:

User Priority	Packet Handling	Max Retries for Packet Discard
CoS 0 (Best Effort)	Reliable	NO DISCARD (0-128)
CoS 1 (Background)	Reliable	NO DISCARD (0-128)
CoS 2 (Spare)	Reliable	NO DISCARD (0-128)
CoS 3 (Excellent)	Reliable	NO DISCARD (0-128)
CoS 4 (Controlled Load)	Reliable	NO DISCARD (0-128)
CoS 5 (Video)	Reliable	NO DISCARD (0-128)
CoS 6 (Voice)	Low Latency	3 (0-128)
CoS 7 (Network Control)	Reliable	NO DISCARD (0-128)

146920

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 the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Once you have defined the retry level, you can also configure the speed at which those frames should be sent. This is done at the bottom of the page, in the **Low Latency Packet Rates** section. You can set each rate to:

- Nominal—The AP will try to use this rate to send the Low Latency Packets (using the faster rate first, and of course depending on the client signal level).
- Non-nominal—The AP will try not to use that rate, but will revert to it if no nominal rate is possible.
- Disabled—The AP will not try to use that rate.

From the CLI, use radio interface config commands as follows (The CLI commands offer more options than the GUI page):

packet max-retries *number 1 number 2 fail-threshold number 3 number 4 priority value drop-packet*

In the previous command:

- Number 1—Defines the number of times the AP should try to resend a packet that was not received properly (not acknowledged), for a given priority level. Once number 1 is reached, the AP drops the packet and tries to send the next one (to the same recipient).
- Number 3—Determines how many consecutive packets (sent to one recipient) can fail before the AP decides that its fail-rate exceeds an acceptable threshold.
- Number 2—Once the fail-threshold is exceeded, the AP may still resend failed packets, but with a different number of attempts than before the threshold is exceeded. This is number 2. For example, you can decide initially to resend each packet 3 times (number 1). Then, if your AP fails to send a certain number of consecutive packets (for example 100, as number 3), you can decide that conditions are degraded, and that your AP should only try to resend each following packet once (which is number 2).
- Number 4—Determines how many more consecutive packets the AP should try to resend with number 2 retries before de-associating the target client.

Example:

```
ap(config-if)# packet max-retries 3 0 fail-threshold 100 500 priority 6 drop-packet
```

In this example, the AP tries to resend each packet of priority level 6 three times (number one = 3). If more than 100 consecutive packets (number three = 100) fail to the same destination, the AP sends each consecutive packet to that destination only once (number two = 0). If 500 more packets (number four = 500) fail to that same destination, the AP disconnects that client.

When using the GUI, number one is defined manually (default is 3). Number 2 defaults to 0, number 3 defaults to 100 and number 4 defaults to 500. These numbers can then be changed from the CLI.

```
ap(config-if)#packet max-retries ?
<0-128> # packet retries before dropping pkt if first fail-threshold not
reached

ap(config-if)#packet max-retries 3 ?
<0-128> # packet retries before dropping pkt if 2nd fail-threshold not
reached

ap(config-if)#packet max-retries 3 0 ?
fail-threshold maximum # consecutive dropped packets thresholds

ap(config-if)#packet max-retries 3 0 fa
ap(config-if)#packet max-retries 3 0 fail-threshold ?
<0-1000> # consecutive dropped packets before switching max-retries
thresholds

ap(config-if)#packet max-retries 3 0 fail-threshold 100 ?
<0-1000> number of consecutive dropped packets before disassociating client

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 ?
priority qos user-priority

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 p
ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority ?
<0-7> qos user-priority number

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 ?
drop-packet Don't retry pkts, just drop packets when max retries reached
```

```
ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 d
ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 drop-packet
```

Low latency Packet rates can also be defined at the interface level, using the following command which defines the nominal rates and the allowed rates to use:

traffic-stream priority value sta-rates {[nominal rates] | [rates]}

```
ap(config-if)# traffic-stream priority 6 sta-rates ?
 12.0      Allow 12.0 Mb/s rate
 18.0      Allow 18.0 Mb/s rate
 24.0      Allow 24.0 Mb/s rate
 36.0      Allow 36.0 Mb/s rate
 48.0      Allow 48.0 Mb/s rate
 54.0      Allow 54.0 Mb/s rate
 6.0       Allow 6.0 Mb/s rate
 9.0       Allow 9.0 Mb/s rate
 nom-12.0  Allow Nominal 12.0 Mb/s rate
 nom-18.0  Allow Nominal 18.0 Mb/s rate
 nom-24.0  Allow Nominal 24.0 Mb/s rate
 nom-36.0  Allow Nominal 36.0 Mb/s rate
 nom-48.0  Allow Nominal 48.0 Mb/s rate
 nom-54.0  Allow Nominal 54.0 Mb/s rate
 nom-6.0   Allow Nominal 6.0 Mb/s rate
 nom-9.0   Allow Nominal 9.0 Mb/s rate
<cr>
```

Example:

```
ap(config-if)# traffic-stream priority 6 sta-rates nom-5.5 nom-11.0 nom-6.0 9.0 nom-12.0
nom-24.0
```

For the voice queue (UP 6 specifically), you can also use the interface command packet speed to determine the rates allowed to use to send packets in the voice queue:

packet speed 5.5 11.0 6.0 9.0 12.0 24.0 priority 6

Notice that the packet speed command focuses on defining the allowed rates, while the command traffic-stream priority also defines the preferred rates among the allowed rates. If you use both commands for the voice queue, the rates defined as nominal in the traffic stream priority command are tried first, then non nominal rates and packet speed rates are attempted.

Configuring ClientLink

Cisco ClientLink (referred to as Beam Forming) is an intelligent beamforming technology that directs the RF signal to 802.11a/g devices to improve performance by 65%, improve coverage by up to 27% percent, and reduce coverage holes.

Cisco ClientLink helps extend the useful life of existing 802.11a/g devices in mixed-client networks and 802.11n clients supporting only one traffic stream. It is beneficial for organizations that move to 802.11n and want to ensure that all clients on the network, regardless of type, are guaranteed the bandwidth and throughput they need.



Note

ClientLink Ver 1 supports 802.11 a/g devices and ClientLink Ver 2 supports 802.11 a/g devices and 802.11n devices with one spatial stream.

**Note**

ClientLink is not supported on the 1040, 702 series access points.

Using the CLI to Configure ClientLink

To enable ClientLink, enter this CLI command in interface configuration mode on 802.11n radio interfaces:

```
beamform ofdm
```

**Note**

Currently the ClientLink configuration option is not available through GUI.

To determine the threshold from which you start doing ClientLink, use the following command:

```
ap(config-if)# beamform rssi 30to128-rssi-threshold-in-dBm
```

ClientLink is disabled by default. Additional details can be found on cisco.com at the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10092/white_paper_c11-516389.html

Debugging Radio Functions

Use the **debug dot11** privileged EXEC command to begin debugging of radio functions. Use the **no** form of this command to stop the debug operation. The command syntax is:

```
[no] debug dot11
{events | packets | forwarding | mgmt | network-map | syslog | virtual-interface}
```

The syntax is described in [Table 6-4](#).

Table 6-4 Syntax for debug dot11 Command

Syntax	Description
events	Activates debugging of all radio related events
packets	Activates debugging of radio packets received and transmitted
forwarding	Activates debugging of radio forwarded packets
mgmt	Activates debugging of radio access point management activity
network-map	Activates debugging of radio association management network map
syslog	Activates debugging of radio system log
virtual interface	Activates debugging of radio virtual interfaces

This example shows how to begin debugging of all radio-related events:

```
AP# debug dot11 events
```

This example shows how to begin debugging of radio packets:

```
AP# debug dot11 packets
```

This example shows how to begin debugging of the radio system log:

```
AP# debug dot11 syslog
```

This example shows how to stop debugging of all radio related events:

```
AP# no debug dot11 events
```

**Note**

Debugging not enabled is the default of the command.

802.11r Configuration

802.11r enables fast roaming across access point in the same subnet using Wireless Domain Service. When you enable 802.11r, a Mobility Domain Information Element (MDIE) is advertised in the AP beacons. The same MDIE is announced by all APs associated to the same WDS. The last 2 bytes of the WDS BVI IP address (IPv4 or Ipv6) is used as MDIE. 802.11r compatible clients use this MDIE to identify APs belonging to the same domain and between which fast roaming is possible.

For a client to move from its current AP to a target AP utilizing the FT protocols, the message exchanges are performed using one of two methods:

- **Over-the-Air**—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm. To set this, use the command:
`ap(config-if)#dot11 dot11r pre-authentication over-air`
- **Over-the-DS**—The client communicates with the target AP via the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP, and is then sent through the WDS to the target AP. To set this, use the command:
`ap(config-if)#dot11 dot11r pre-authentication over-ds`

On an AP radio, you can enable 802.11r support, and decide if roaming dialog should occur over the air (default) or over the DS, and also configure the maximum time allowed for a client to complete the roaming transaction. The maximum time allowed for a client to complete the roaming transaction is called Re-association Timer. This timer allows you to add security to your network by preventing attackers from opening many 802.11r transactions without completing any of them, which can overload the AP. You can set this timer using the following command:

```
ap(config-if)#dot11 dot11r reassociation-time value 20to1200-timeout-value-in-milli-seconds
```

Example:Enable 802.11r, with authentication over the DS, and re-association time value of 200 ms.

```
aap(config-if)#dot11 dot11r pre-authentication over-ds  
ap(config-if)#dot11 dot11r reassociation-time value 200
```

**Note**

Test 802.11r before implementing it into your network. Some non-802.11r clients do not support 802.11r MDIE and do not operate well in 802.11r environments.

Setting Traffic Rate Limits for an SSID and Radio Interface

To limit the bandwidth usage by wireless client devices, you can limit the traffic rate to and from wireless client devices. This rate limiting feature can be:

- Configured for each SSID and can be applied on one or both radio interfaces
- Applied only to TCP/UDP on IPv4. Not supported for IPv6 traffic.
- Applied to both input (ingress) and output (egress) traffic on a radio interface

The rate limiting feature is available for VLANs. If you have more than one SSID configured on the same interface, then you cannot configure rate limits without having VLANs.

For information on configuring multiple SSIDs, see [Chapter 7, “Configuring Multiple SSIDs”](#).

For information on VLANs, see [Chapter 14, “Configuring VLANs”](#).

As part of Quality of Service (QoS) feature, a rate limiting feature which limits the input or output transmission rate of a class of traffic based on user-defined criteria is present. See [Chapter 15, “Configuring QoS”](#), for more information on that.

Configuring Rate Limits

To configure the rate limits, use the command

rate-limit {tcp | udp} {input | output} data-rate rate burst-size size, where;

- Date-rate is the average rate of data transmission, specified in Kilobits/sec.
- Burst-size is the total data that can be transmitted before the traffic is throttled. It is specified in Kilobits.

These parameters are converted and limited to the nearest multiple of 8, whereby data-rate is converted to KiloBytes/sec and burst-size is converted to Bytes, and then are considered for rate limiting.

To understand how these parameters work, follow this example. Consider the average data rate as 10 Bytes/sec and the burst-size as 20 Bytes. Then the rate limit applied here is such that in a duration of 2 seconds (calculated as Burst-size/Average Rate) the total data transmission is not allowed to exceed 20 Bytes. This also allows for more data to be transmitted per second as long the average data-rate does not exceed 10 Bytes/sec.

To configure via the GUI, go to **Security > SSID Manager**. Under the **Rate Limit Parameters** section, you can limit input or output traffic for TCP or UDP, as required. You can also specify the rate and burst-size in each case.

Viewing the Rate Limit Statistics

To view the statistics of rate limits, for each ssid configured on a given interface, use the command **show interface dot11radio {0 | 1} qos-info**

To clear the statistics counters, use the command **clear counters dot11Radio {0 | 1}**

To view the rate limit statistics via the GUI, go to **Network > Network Interface > Radio0-802.11N 2.4GHz** or **Radio1-802.11N 5GHz**. To clear the statistics, click **Clear**.