



Dynamic Frequency Selection

At startup and by default, wireless devices passively scan for and select the least-congested channel. The channel settings on wireless devices correspond to the frequencies available in your regulatory domain.

For example, in the European Telecommunications Standards Institute (ETSI) domain, the regulatory agencies do not allow the channel to be set on 5.0 GHz (802.11a/h) radios by the users. However, channel groups can be *blocked* on wireless devices running ETSI images. When a wireless device boots from an ETSI image, it automatically selects the least congested channel where radar is not detected by using Dynamic Frequency Selection (DFS).

Transmission Power Control (TPC) is used to automatically adjust the transmission power level on 5.0-GHz radios, also to avoid interfering with radar.

Understanding Dynamic Frequency Selection

TPC is used to automatically adjust the transmission power level on 5.0-GHz radios, also to avoid interfering with radar. 5.0 GHz (802.11a/h) radios in wireless devices running Cisco IOS version 12.4(6)T and later shipped to Europe and Japan are required to use DFS to detect and avoid interfering with radar signals to comply with those regulatory domains.

DFS is the process of detecting radar signals that must be protected against interference from 5.0 GHz (802.11a/h) radios, and upon detection switching the operating frequency of the 5.0 GHz (802.11a/h) radio to one that is not interfering with the radar systems. TPC is used to adapt the transmission power of a radio based on regulatory requirements and range information.

The wireless device automatically sets the frequency on a DFS-enabled 5.0 GHz (802.11a/h) radio operating in a regulatory domain where DFS is required for compliance with the rules of that regulatory agency.

For the ETSI regulatory domain, 5.0-GHz radios support the DFS 1.3.1 compliance requirement.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

DFS Actions

DFS-enabled radios monitor the operating frequency for radar signals. If radar signals are detected on the channel, the wireless device takes these steps:

- Blocks new transmissions on the channel.
- Flushes the power-save client queues.¹
- Broadcasts an 802.11h channel-switch announcement.
- Disassociates remaining client devices.
- Randomly selects a different channel:
 - If the wireless device does not select a DFS-required channel, it enables beacons and accepts client associations.
 - If the wireless device selects a DFS-required channel, it scans the new channel for radar signals for 60 seconds. If there are no radar signals on the new channel, the wireless device enables beacons and accepts client associations. If a radar signal is detected, the wireless device selects a different channel.

If a preferred channel is configurable and available, it is selected first.

Dynamic Frequency Selection Channels

When a DFS-enabled radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

- 52 (5260 MHz)
- 56 (5280 MHz)
- 60 (5300 MHz)
- 64 (5320 MHz)
- 100 (5500 MHz)
- 104 (5520 MHz)
- 108 (5540 MHz)
- 112 (5560 MHz)
- 116 (5580 MHz)
- 120 (5600 MHz)
- 124 (5620 MHz)
- 128 (5640 MHz)
- 132 (5660 MHz)
- 136 (5680 MHz)
- 140 (5700 MHz)

1. 52, (5260 MHz), 64 (5320 MHz), 120 (5600 MHz), and 128 (5640) are not supported on the Cisco 3200 Series WMIC.

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.

Configuring a Preferred Channel

By default, a WMIC in the root mode randomly selects its operating channel to meet the uniform channel distribution requirement for standalone deployments. However, the random selection of the operating channel can result in adjacent and co-channel interference in deployments with multiple overlapping access points.

To minimize this type of interference, specify the channel of operation (prefer channel) of each access point. The user is then responsible for ensuring that the selected channels are uniformly distributed across the network.

To configure a prefer channel for the C3205 WMIC 12.3(2)JL release, use the following command:

```
spacing {5 | 10 | 20} channel prefer_channel [return-time <1-48>]
```

To configure a prefer channel for the C3205 WMIC 12.4(3g)JK release, use the following command:

```
channel prefer_channel [return-time <1-48>]
```

These commands let you specify a *prefer* channel for the WMIC to use as its operating channel. The commands mark the specified channel with the highest priority to be chosen, but not the only channel that can be used.

After the prefer channel is configured, the WMIC resets its radio and selects the configured prefer channel to go through the channel availability check (60 seconds of scanning for radar signals) prior to enabling transmission on the channel.

However, if a radar signal is detected on the prefer channel, a new operating channel is randomly selected, which again can result in interchannel interference.

To resolve this issue, you can use the **return-time** option to specify a timeout period. This forces the WMIC to periodically try to return to the configured prefer channel after the timeout period expires, provided no radar is operating on the channel. If radar is operating on the prefer channel, the WMIC tries again after another timeout period expires. The WMIC keeps trying until it finds no radar on the prefer channel, at which point the WMIC switches back to the prefer channel.

To specify a prefer channel and configure a timeout period do the following.

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface dot11radio port	Enters interface configuration mode for the radio interface.
Step 3	channel <i>prefer_channel</i> [return-time <i>timeout_period</i>]	Specifies the prefer channel. (Optional) Specifies in 30-minute time units how long to wait before trying to return to the prefer channel after radar has been detected on the operating prefer channel. The minimum value is 1 time unit (30 minutes). The maximum value is 48 time units (1,440 minutes or 24 hours). The default value is 1 (30 minutes).
Step 4	end	Returns to privileged EXEC mode.

The WMIC sends an SNMP management trap whenever a channel is switched due either to radar detection or a return to the prefer channel.

Configuring Radar Detection By Clients

By default, radar detection is disabled in the workgroup bridge and non-root bridge modes (client modes). However, you can use the **radar-detection-enabled** command in the workgroup bridge or non-root bridge mode to enable radar detection in the client mode.

radar-detection-enabled [dot11h | iapp]

The default notification method is **dot11h** (802.11h). However, you can specify Inter-Access Point Protocol (IAPP) as the notification method. IAPP is also known as IEEE 802.11F.

After a wireless device in client mode associates with a root device, it checks whether radar detection is enabled and whether the current uplink channel is a DFS channel. If radar detection is enabled and the current uplink channel is a DFS channel, the wireless device in client mode enables radar detection for this channel.

When the wireless device detects a radar signal, it immediately notifies the root device, brings down its interface, and restarts uplink scanning.

When the root device receives radar detection notification from a client, it check the association status:

- If the client is associated and authenticated, the root device immediately responds to the client's radar detection notification by marking the channel specified by the client as a radar channel and switches to a new channel following the channel availability check.

In addition, the root device sends an SNMP trap to the network administrator.

- If the client is not authenticated or associated to the root device, the root device silently drops the client's notification.

Configuring an SNMP Trap for Radar Detection



Note

This command is available on the Cisco 3205 WMIC only.

To configure an SNMP trap for radar detection or to switch to prefer channel notification, use the **snmp-server enable traps** command on the master (root) device.

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	snmp-server enable traps { channel-return channel-switch }	Specifies whether to send a notification when the WMIC returns to the prefer channel or switches to a randomly selected channel because of radar detection.
Step 3	end	Returns to privileged EXEC mode.

Additional Information

For general information on channel selection and transmit power, see the “FCC Regulations Update For 2004” white paper at:

http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_white_paper0900aecd801c4a88.shtml

Additional information on DFS and TPC can be found in the Cisco “Dynamic Frequency Selection and IEEE 802.11h Transmit Power Control” document available at:

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008060f7c2.html

For additional information on the 4.9 GHz (public safety) band, see the “Cisco Support for 4.9 GHz Public Safety Broadband Spectrum in the US” white paper at:

http://www.cisco.com/en/US/products/hw/routers/ps272/prod_brochure0900aecd802d81

