Radio Bands

802.11 Bands

You can configure the 802.11b/g/n (2.4 GHz) and 802.11a/n/ac (5 GHz) bands for the controller to comply with the regulatory requirements in your country. By default, both 802.11b/g/n and 802.11a/n/ac are enabled.

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully connect to an access point, but cannot pass traffic. When you configure the controller only for 802.11g traffic, you must mark 11g rates as mandatory.

Note The Block Acks in a Cisco 2800, 3800, 1560 APs are sent at configured mandatory data rates in controller for 2.4 GHz radio.

This section contains the following subsections:

Configuring the 802.11 Bands (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network** to open the **Global Parameters** page.

Step 2 Select the **802.11a** (or **802.11b/g**) **Network Status** check box to enable the 802.11a or 802.11b/g band. To disable the band, unselect the check box. The default value is enabled. You can enable both the 802.11a and 802.11b/g bands.

Step 3 If you enabled the 802.11b/g band in *Step 2*, select the **802.11g Support** check box if you want to enable 802.11g network support. The default value is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

Step 4 Specify the period at which the SSID is broadcast by the access point by entering a value between 20 and 1000 milliseconds (inclusive) in the Beacon Period text box. The default value is 100 milliseconds.

Note The beacon period in controllers is listed in terms of milliseconds. The beacon period can also be measured in time units, where one time unit equals 1024 microseconds or 102.4 milliseconds. If a beacon interval is listed as 100 milliseconds in a controller, it is only a rounded off value for 102.4 milliseconds. Due to hardware limitation in certain radios, even though the beacon interval is, say 100 time units, it is adjusted to 102 time units, which roughly equals 104.448 milliseconds. When the beacon period is to be represented in terms of time units, the value is adjusted to the nearest multiple of 17.

Step 5 Specify the size at which packets are fragmented by entering a value between 256 and 2346 bytes (inclusive) in the Fragmentation Threshold text box. Enter a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 6 Make access points advertise their channel and transmit power level in beacons and probe responses for CCX clients. Select the **DTPC Support** check box. Otherwise, unselect this check box. The default value is enabled.

Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

Note On access points that run Cisco IOS software, this feature is called *world mode*.

Note DTPC and 801.11h power constraint cannot be enabled simultaneously.

Step 7 Specify the maximum allowed clients by entering a value between 1 to 200 in the Maximum Allowed Client text box. The default value is 200.

Step 8 Select or unselect the **RSSI Low Check** check box to enable or disable the RSSI Low Check feature.

Step 9 Enter the **RSSI Threshold** value.

The default value is –80 dBm.

Step 10 Use the Data Rates options to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:

- 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps
- 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

For each data rate, choose one of these options:

- **Mandatory**—Clients must support this data rate in order to associate to an access point on the controller.
- **Supported**—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- **Disabled**—The clients specify the data rates used for communication.

Step 11 Click **Apply**.

Step 12 Click **Save Configuration**.

Configuring the 802.11 Bands (CLI)

Procedure

Step 1 Disable the 802.11a band by entering this command:

config 802.11a disable network

Note The 802.11a band must be disabled before you can configure the 802.11a network parameters in this section.

Step 2 Disable the 802.11b/g band by entering this command:

config 802.11b disable network

Note The 802.11b band must be disabled before you can configure the 802.11b network parameters in this section.

Step 3 Specify the rate at which the SSID is broadcast by the access point by entering this command:

config {**802.11a** | **802.11b**} **beaconperiod** *time_unit*

where *time_unit* is the beacon interval in time units (TUs). One TU is 1024 microseconds. You can configure the access point to send a beacon every 20 to 1000 milliseconds.

Step 4 Specify the size at which packets are fragmented by entering this command:

config {**802.11a** | **802.11b**} **fragmentation** *threshold*

where *threshold* is a value between 256 and 2346 bytes (inclusive). Specify a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 5 Make access points advertise their channel and transmit power level in beacons and probe responses by entering this command:

config {**802.11a** | **802.11b** } **dtpc** {**enable** | **disable**}

The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

Note On access points that run Cisco IOS software, this feature is called *world mode*.

Step 6 Specify the maximum allowed clients that can be configured by entering this command:

config {**802.11a** | **802.11b**} **max-clients** *max_allow_clients*

The valid range is between 1 to 200.

Step 7 Configure the RSSI Low Check feature by entering this command:

config 802.11{**a** | **b**} **rssi-check** {**enable** | **disable**}

Step 8 Configure the RSSI Threshold value by entering this command:

config 802.11{**a** | **b**} **rssi-threshold** *value-in-dBm*

Note The default value is –80 dBm.

Step 9 Specify the rates at which data can be transmitted between the controller and the client by entering this command:

config {**802.11a** | **802.11b**} **rate** {**disabled** | **mandatory** | **supported**} *rate*

where

- **disabled**—Clients specify the data rates used for communication.
- **mandatory**—Clients support this data rate in order to associate to an access point on the controller.
- **supported**—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- *rate*—The rate at which data is transmitted:
  - 6, 9, 12, 18, 24, 36, 48, and 54 Mbps (802.11a)
  - 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps (802.11b/g)

Step 10 Enable the 802.11a band by entering this command:

config 802.11a enable network

The default value is enabled.

Step 11 Enable the 802.11b band by entering this command:

config 802.11b enable network

The default value is enabled.

Step 12 Enable or disable 802.11g network support by entering this command:

config 802.11b 11gSupport {**enable** | **disable**}

The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

Step 13 Enter the **save config** command to save your changes.

Step 14 View the configuration settings for the 802.11a or 802.11b/g band by entering this command:

show {**802.11a** | **802.11b**}

Information similar to the following appears:

```
802.11a Network.............................. Enabled
11nSupport................................... Enabled
      802.11a Low Band....................... Enabled
      802.11a Mid Band....................... Enabled
      802.11a High Band...................... Enabled
802.11a Operational Rates
    802.11a 6M Rate.......................... Mandatory
    802.11a 9M Rate.......................... Supported
    802.11a 12M Rate......................... Mandatory
    802.11a 18M Rate......................... Supported
    802.11a 24M Rate......................... Mandatory
    802.11a 36M Rate......................... Supported
```

```
    802.11a 48M Rate.............................. Supported
    802.11a 54M Rate.............................. Supported
...
Beacon Interval.................................. 100
...
Default Channel.............................. 36
Default Tx Power Level....................... 1
DTPC Status.................................. Enabled
Fragmentation Threshold...................... 2346
Maximum Number of Clients per AP................. 200
```

802.11n Parameters

This section provides instructions for managing 802.11n access points on your network. The 802.11n devices support the 2.4 and 5-GHz bands and offer high throughput data rates.

The 802.11n high throughput rates are available on all the 802.11n access points for the WLANs using WMM with no Layer 2 encryption or with WPA2/AES encryption enabled.

The 802.11n-only access points can filter out clients without high-throughput information element on the association request. The 802.11n-only access points access points reject association requests from clients without high-throughput information element (11n).

In the 802.11n high-throughput mode, there are no 802.11a/b/g stations using the same channel. The 802.11a/b/g devices cannot communicate with the 802.11n high-throughput mode access point, where as the 802.11n-only mode access point uses 802.11a/g rates for beacons or management frames.

Note Some Cisco 802.11n APs may intermittently emit incorrect beacon frames, which can trigger false wIPS alarms. We recommend that you ignore these alarms.

Configuring the 802.11n Parameters (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **High Throughput** to open the (5 GHz or 2.4 GHz) High Throughput page.

Step 2 Select the **11n Mode** check box to enable 802.11n support on the network. The default value is enabled.

If you want to disable 802.11n mode when both 802.11n and 802.11ac modes are enabled, you must disable the 802.11ac mode first.

Step 3 Select the check boxes of the desired rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. These data rates, which are calculated for a 20-MHz channel width using a short guard interval, are available:

- 0 (7 Mbps)

- 1 (14 Mbps)
- 2 (21 Mbps)
- 3 (29 Mbps)
- 4 (43 Mbps)
- 5 (58 Mbps)
- 6 (65 Mbps)
- 7 (72 Mbps)
- 8 (14 Mbps)
- 9 (29 Mbps)
- 10 (43 Mbps)
- 11 (58 Mbps)
- 12 (87 Mbps)
- 13 (116 Mbps)
- 14 (130 Mbps)
- 15 (144 Mbps)

  Any associated clients that support the selected rates may communicate with the access point using those rates. However, the clients are not required to be able to use this rate in order to associate. The MCS settings determine the number of spatial streams, the modulation, the coding rate, and the data rate values that are used.

- 16 (22 Mbps)
- 17 (43 Mbps)
- 18 (65 Mbps)
- 19 (87 Mbps)
- 20 (130 Mbps)
- 21 (173 Mbps)
- 22 (195 Mbps)
- 23 (217 Mbps)
- 24 (29 Mbps)
- 25 (58 Mbps)
- 26 (87 Mbps)
- 27 (116 Mbps)
- 28 (173 Mbps)
- 29 (231 Mbps)

- 30 (260 Mbps)
- 31 (289 Mbps)

Step 4 Click **Apply**.

Step 5 Use the 802.11n data rates that you configured by enabling WMM on the WLAN as follows:

a) Choose **WLANs** to open the WLANs page.
b) Click the ID number of the WLAN for which you want to configure WMM mode.
c) When the WLANs > Edit page appears, choose the **QoS** tab to open the WLANs > Edit (Qos) page.
d) From the WMM Policy drop-down list, choose **Required** or **Allowed** to require or allow client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

If you choose **Allowed**, devices that cannot support WMM can join the WLAN but will not benefit from the 802.11n rates.

e) Click **Apply**.

Step 6 Click **Save Configuration**.

Note To determine if an access point supports 802.11n, look at the 11n Supported text box on either the 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page or the 802.11a/n/ac (or 802.11b/g/n) AP Interfaces > Details page.

Configuring the 802.11n Parameters (CLI)

Procedure

- Enable 802.11n support on the network by entering this command:

  config {**802.11a** | **802.11b**} **11nsupport** {**enable** | **disable**}

- Specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client by entering this command:

  config {**802.11a** | **802.11b**} **11nsupport mcs tx** {**0-15**} {**enable** | **disable**}

- Use the 802.11n data rates that you configured by enabling WMM on the WLAN as follows:

  config wlan wmm {**allow** | **disable** | **require**} *wlan_id*

  The **require** parameter requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

  If set to **allow**, devices that cannot support WMM can join the WLAN but do not benefit from 802.11n rates.

- Specify the aggregation method used for 802.11n packets as follows:
  a) Disable the network by entering this command:

     config {**802.11a** | **802.11b**} **disable network**

  b) Specify the aggregation method entering this command:

     config {**802.11a** | **802.11b**} **11nsupport** {**a-mpdu** | **a-msdu**} **tx priority** {**0-7** | **all**} {**enable** | **disable**}

Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). A-MSDU is performed in hardware and therefore is the default method.

Note For 802.11ac, all packets are A-MPDU. The A-MSDU option does not apply for 802.11ac.

You can specify the aggregation method for various types of traffic from the access point to the clients. This table defines the priority levels (0-7) assigned per traffic type.

Table 1: Traffic Type Priority Levels

User Priority	Traffic Type
0	Best effort
1	Background
2	Spare
3	Excellent effort
4	Controlled load
5	Video, less than 100-ms latency and jitter
6	Voice, less than 10-ms latency and jitter
7	Network control

You can configure each priority level independently, or you can use the **all** parameter to configure all of the priority levels at once. When you use the **enable** command, the traffic associated with that priority level uses A-MPDU transmission. When you use the **disable** command, the traffic associated with that priority level uses A-MSDU transmission. Configure the priority levels to match the aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4 and 5 and the rest are disabled. By default, A-MSDU is enabled for all priorities except 6 and 7.

c) Reenable the network by entering this command:

config {**802.11a** | **802.11b**} **enable network**

- Configure the 802.11n-5 GHz A-MPDU transmit aggregation scheduler by entering this command:

  config 802.11{**a** | **b**} **11nsupport a-mpdu tx scheduler** {**enable** | **disable** | **timeout rt** *timeout-value*}

  The timeout value is in milliseconds. The valid range is between 1 millisecond to 1000 milliseconds.

- Configure the guard interval for the network by entering this command:
  config 802.11{**a** | **b**} **11nsupport guard_interval** {**any** | **long**}
- Configure the Reduced Interframe Space (RIFS) for the network by entering this command:

  config 802.11{**a** | **b**} **11nsupport rifs rx** {**enable** | **disable**}

- Save your changes by entering this command:

save config

- View the configuration settings for the 802.11 networks by entering this command:

  show {**802.11a** | **802.11b**}

802.11ac Parameters

The 802.11ac radio module for the Cisco Aironet 3600 Series access point and Cisco Aironet 3700 Series access point provides enterprise-class reliability and wired-network-like performance. It supports three spatial streams and up to 160 MHz-wide channels for a maximum data rate of 2.5 Gbps.

The 802.11ac radio in slot 2 is a subordinate radio for which you can configure specific parameters. Because the 802.11ac is a subordinate radio, it inherits many properties from the main 802.11a/n radio on slot 1. The parameters that you can configure for the 802.11ac radio are as follows:

- Admin status—Interface status of the radio that you can enable or disable. By default, the Admin status is in an enabled state. If you disable 802.11n, the 802.11ac radio is also disabled.
- Channel width—You can choose the RF channel width as 20 MHz, 40 MHz, 80 MHz, or 160 MHz. If you choose the channel width as 160 MHz, you must enable the 802.11ac mode on the **High Throughput** page.

Note The **11ac Supported** field is a nonconfigurable parameter that appears for the 802.11ac subordinate radio in slot 2.

Note When the Cisco Aironet 3600 Series access point with 802.11ac radio module is in unsupported mode such as Monitor and Sniffer, Admin Status and Channel Width will not be configured.

This section provides instructions to manage 802.11ac devices such as the Cisco Aironet 3600 Series Access Points and Cisco Aironet 3700 Series Access Point on your network.

Note For the Cisco Aironet 3600 Series APs:

- With default AP group—Only WLAN IDs 1 to 8 are advertised on the 5-GHz radios; there is no limit on the 2.4-GHz radios.
- With user-defined AP group—Only the first 8 WLAN IDs are advertised on the 5-GHz radios regardless of the ID number; there is no limit on the 2.4-GHz radios.

Changing the 802.11n radio channel also changes the 802.11ac channels.

On the Cisco WLC GUI, the 802.11ac clients that are connected to the 802.11n radio are displayed 802.11an clients, and the 802.11ac clients that are connected to the 802.11ac radio are displayed as 802.11ac clients.

Ensure that your WLAN has WMM enabled and open or WPA2/AES for 802.11ac to be supported. Otherwise, the speed of 802.11ac is not available, even on 802.11ac clients.

For more information about the 802.11ac module on the Cisco Aironet 3600 Series access point, see http://www.cisco.com/c/en/us/products/wireless/aironet-3600-series/relevant-interfaces-and-modules.html.

802.11ac Wave 2 and MU-MIMO

The 802.11ac Wave 2 introduces additional capabilities beyond what were added with Wave 1. It utilizes MU-MIMO technology and other advancements to help increase wireless performance for applications such as HD video streaming. Wave 2 provides better RF efficiency that Wave 1 provides, in addition to a number of other features that further improve wireless connectivity.

MU-MIMO

MU-MIMO is short for Multi-User, Multiple-Input, Multiple-Output. MU-MIMO is an enhanced form of the MIMO technology that enables multiple independent radio terminals to access a system.

With 802.11n or 802.11ac Wave 1, an access point can transmit multiple spatial streams at the same time, but only directed to a single wireless client. This means only a single device gets data at a time. This is referred to as single-user MIMO (SU-MIMO).

802.11ac Wave 2 allows for MU-MIMO, which enables multiple users to simultaneously receive data from the AP simultaneously using the same channel. With MU-MIMO a Wave 2 capable access point is able to use its antenna resources to transmit to multiple clients, all at the same time and over the same channel. MU-MIMO is used in the downstream direction and requires the wireless clients to also be Wave 2 capable.

More Spatial Streams

802.11ac Wave 2 allows for up to eight spatial streams. However, initial Wave2 implementations will only increase the number of spatial streams from 3 to 4 as compared to Wave 1 implementations. The support of an additional spatial stream allows for additional increased performance as compared to 3 SS APs.

References

For more information on these technologies, see the following documents on Cisco.com:

- *Cisco 802.11ac Wave 2 FAQs* at http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11ac-solution/q-and-a-c67-734152.html
- *Fundamentals of 802.11ac Wave 2 post on the Cisco Interaction Network* at http://blogs.cisco.com/cin/fundamentals-of-802-11ac-wave-2
- *802.11ac: The Fifth Generation of Wi-Fi* technical white paper at http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.html

Explicit Compressed Beamforming Feedback

The AP 1850 supports standards-based Explicit Compressed Beamforming Feedback (ECBF) as defined in the 802.11ac standards. With ECBF the client provides estimates of the wireless channel conditions to the access point. As these are based on explicit channel measurements from the client, both the AP and the client must support it. For 802.11ac, the access point's ECBF is typically referred to as Transmit Beamforming or TxBF for short.

While both TxBF and ClientLink 3.0 improve the performance of wireless client devices, ClientLink3.0 provides an additional advantage over TxBF. ClientLink3.0 technology does not depend on any client-side hardware or software capabilities and operates seamlessly in mixed-mode environments where 802.11ac and 802.11a/n clients coexist on the same access point. In comparison, TxBF requires client-side support to take advantage of the performance improvements of beamforming and therefore benefits only 802.11ac clients that support TxBF.

The Cisco 1850 AP supports TxBF but not beamforming to legacy client devices. Therefore, Cisco 1850 AP does not support ClientLink 3.0.

Note ClientLink 3.0 is supported on the Cisco Aironet 2700 and 3700 Series 802.11ac APs.

Note You can disable TxBF only on the APs that support ClientLink 1.0. It cannot be disabled on the APs that supports ClientLink 2.0 and above.

Restrictions for 802.11ac Support

- The 802.11ac module is supported only on the following access points:
  - 1700
  - 1800
  - 2700
  - 2800
  - 3700
  - 3800
- The 802.11ac module is turned off if the built-in 5-GHz radio is turned off.
- You must ensure that the configuration of the channel, power values, and the mode of the 802.11ac module is the same as those of the built-in 5-GHz radio on the AP. Also, the 802.11ac module serves only 802.11ac clients.
- The 802.11ac module main channel cannot be changed individually.
- This 802.11ac support is applicable only to the following controller platforms:
  - Cisco 3504 WLC
  - Cisco 5520 WLC
  - Cisco 8540 WLC
- Controllers do not support High availability for 802.11ac modules. The 802.11ac configuration (802.11ac Data Rates and 802.11ac Global mode) on the controller is not synchronized with the standby controller. This might result in client throughput fluctuations and reassociations when you explicitly disable those configurations on the active controller.

  In addition, the 802.11ac Global mode configuration controls whether the radio module is enabled. If 802.11ac Global mode is enabled on one controller but not on another, the 802.11ac module might be disabled if the access point associates with a controller on which 802.11ac Global mode is disabled.

- When changing AP from static to auto channel assignment, by default AP moves to best possible bandwidth supported by the radio and a valid channel. Channel number and width assignment may be suboptimal until next DCA cycle gets started.
- SSIDs with TKIP and SSIDs with TKIP+AES are not enabled on the 802.11ac radios. Therefore, all the 5-GHz clients are expected to associate with the 802.11n radios.

Configuring the 802.11ac High-Throughput Parameters (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a/n/ac** > **High Throughput (802.11n/ac)**.

Step 2 Check the **11ac mode** check box to enable the 802.11ac support on the network.

Note You can modify the 802.11ac status only if the 802.11n mode is enabled.

Step 3 Ensure that all of the 0 to 31 MCS data rate indices are enabled (which is the default setting).

Step 4 Save the configuration.

Configuring MU-MIMO (GUI)

This feature is supported on all the supporting Cisco Wave 2 APs.

Procedure

Step 1 Choose **WLANs** and click the WLAN ID.

Step 2 In the **Advanced** tab, check or uncheck the **11ac MU-MIMO** check box.

Step 3

Configuring the 802.11ac High-Throughput Parameters (CLI)

Procedure

- Enable or disable 802.11ac support by entering this command:

  config 802.11a 11acSupport {**enable** | **disable**}

- Configure MCS transmit rates by entering this command:

  config 802.11a 11acSupport mcs tx {*rate-8* | *rate-9*} **ss** *spatial-stream-value* {**enable** | **disable**}

Note Ensure that all of the 0 to 31 MCS data rate indices are enabled (which is the default setting). In 8.1 and later releases, RF profiles should include MCS 0-31 instead of MCS 0-23 in earlier releases.

Configuring MU-MIMO (CLI)

This feature is supported on all the Cisco Wave 2 APs.

Procedure

Step 1 Enable or disable MU-MIMO by entering this command on the Cisco WLC console:
config wlan mu-mimo {**enable** | **disable**} *wlan-id*

Step 2 See the status of MU-MIMO by entering these commands on the AP console:

- For a WLAN: **show interfaces Dot11Radio** *Dot11-radio-interface-number* **mumimo wlan** *wlan-id*
- For a client: **show interfaces Dot11Radio** *Dot11-radio-interface-number* **mumimo client** *mac-addr*