Wireless Tab

The Wireless tab on the menu bar provides access to the Cisco WLAN Solution wireless network configuration. Use the left navigation pane to access specific wireless network parameters. Making this selection from the menu bar opens the All APs page.

You can access the following pages from the Wireless tab:

- All APs
- Load Balancing
- Band Select
- Preferred Calls
- SIP Snooping
- Rx SOP Threshold
- Optimized Roaming
- 802.11a/n/ac Radios
- 802.11b/g/n Radios
- Dual-Band Radios
- Global Configuration
- Mesh
- RF Profiles
- FlexConnect Groups
- FlexConnect ACLs
- 802.11a/n/ac Global Parameters
- 802.11a/n/ac RF Grouping
- 802.11a/n/ac Tx Power Control
- 802.11a/n/ac Dynamic Channel Assignment
- 802.11a/n/ac Coverage Hole Detection
- 802.11a/n/ac RRM
- 802.11a/n/ac Client Roaming
- 802.11a/n/ac Voice Parameters
- 802.11a/n/ac Video Parameters

- 802.11a/n/ac Media Parameters
- 802.11 EDCA Parameters
- 802.11h Global Parameters
- 802.11n/ac (5 GHz) Very High Throughput
- 802.11a/n/ac CleanAir
- 802.11b/g/n Global Parameters
- 802.11b/g/n RF Grouping
- 802.11b Tx Power Control
- 802.11b Dynamic Channel Assignment
- 802.11b Coverage Hole Detection
- 802.11b RRM
- 802.11b/g Client Roaming
- 802.11b/g Client Roaming
- 802.11b/g Voice Parameters
- 802.11b/g/n Video Parameters
- 802.11b/g Media Parameters
- 802.11b/g EDCA Parameters
- 802.11n (2.4 GHz) High Throughput
- Configuring Media Stream
- Media Streams
- Application Visibility and Control
- Country
- Timers
- NetFlow
- QoS Profiles
- QoS Roles for Guest Users

All APs

Choose **WIRELESS > Access Points > All APs** or **MONITOR > Summary** and click **All APs** under the AP Summary section to navigate to the All APs page.

This page displays the access points associated with the Cisco WLC. This section consists of the following topics:

- All APs Details
- VLAN Mappings for FlexConnect Access Points
- WebAuth and WebPolicy ACL Mappings for FlexConnect Access Points
- VLAN Mappings for Mesh Access Points
- Neighbor Information of Access Points

- Access Points Statistics

Search AP Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

The current filter parameters are displayed in the Current Filter field.

- MAC Address—MAC address.

> **Note**   When you enable the MAC address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC address filter is disabled automatically.

- AP Name—Access point name. If you do not know the exact name of the AP, you can specify the name partially by entering one or more successive characters that are part of the AP name.
- AP Model—Access point model check box where you select and enter the model of the access point.
- Operating Status—Operating status of the access points:
  - UP—The access point is up and running.
  - DOWN—The access point is not operational.
  - REG—The access point is registered to the controller.
  - DEREG—The access point is not registered to the controller.
  - DOWNLOAD—The controller is downloading its software image to the access point.
- Admin Status—Whether the access points are enabled or disabled on the controller.
- AP Mode—Options to specify the operating mode of the access points: Local, FlexConnect, REAP, Monitor, Rogue Detector, Sniffer, Bridge, and SE Connect. Depending on the capabilities and support available for the APs, one or more options are displayed.

> **Note**   The Cisco OEAP 600 Series access point uses Local mode and the settings cannot be altered. The Cisco OEAP 600 Series access point does not support the following AP Modes: Monitor, FlexConnect, Sniffer, Rogue Detector, Bridge, and SE Connect.

> **Note**   To configure an access point for wIPS, you must set the AP mode to one of the following from the AP Mode drop-down list: Local, FlexConnect, and Monitor.

- Certificate Type—Check boxes that you can select to specify the types of certificates installed on the access points:
  - MIC—Manufactured-installed certificate
  - SSC—Self-signed certificate
  - LSC—Local significant certificate
- Primary S/W Version—Primary software version.
- Secondary S/W Version—Secondary software version.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the All APs page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0, AP Name:pmsk-ap, Operational Status:UP, Status: Enabled, and so on).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

All APs Summary

This table describes the AP parameters.

Table 5-1   *All APs Summary Parameters*

Parameter	Description
AP Name	Operator-defined name of the access point.
IP Address (IPv4/IPv6)	The IPv4/IPv6 address of the AP. From Release 8.0, Cisco WLC supports IPv6.
AP Model	Access point model name.
AP MAC	MAC address of the access point.
AP Up Time	Amount of time that the access point has been powered up.
Admin Status	Administration state of the access point.
Operational Status	Operational status of the access point that is either registered (REG) or not registered (DEREG).
PoE Status	The power level at which the access point is operating: High (20 W), Medium (16.8 W), or Medium (15.4 W). The controller auto-detects the access point's power source and displays the power level.
No: Of Clients	The maximum number of clients to be allowed per AP.
Port	Access point port number.
AP Mode	Access point mode of operation: • Local • FlexConnect • Monitor • Rogue Detector • Sniffer • Bridge • SE Connect **Note** Depending on the capabilities and support available for the APs, one or more of the above options are displayed.

Table 5-1   All APs Summary Parameters

Parameter	Description
Certificate Type	Type of certificate: • MIC (manufactured-installed certificate) • SSC (self-signed certificate) • LSC (local significant certificate)
OEAP (OfficeExtend AP)	Whether this access point is an OfficeExtend access point.
Primary SW Version	Primary image software version available in the access point.
Backup SW Version	Backup image software version available in the access point.
AP Sub Mode	• AP Sub Mode field that shows wIPS if the access point in is monitor mode and the wIPS submode is configured on the access point. • None is displayed if the access point is in local/FlexConnect mode and wIPS submode is not configured. **Note** wIPS ELM is not supported on 1130 and 1240 access points.
Download Status	Download status of the upgrade image on this access point.
Upgrade Role (Master/Slave)	Role of the access point in the upgrade process. Valid values are **Master** and **Slave**.
mDNS Status	Status of mDNS.

For details on a particular access point, click the access point name to open the All APs Details page for that access point.

To view statistics for an access point in Bridge AP mode, click the blue arrow adjacent the desired access point and choose **Statistics**. The Access Points Statistics page for the selected access point appears.

To view neighbor statistics for an access point in Bridge AP mode, click the blue arrow adjacent the desired access point and choose **Neighbor Information**. The Neighbor Information of Access Points page for the selected access point appears.

All APs Details

Choose **WIRELESS > Access Points > All APs** and then click an AP name to navigate to the AP Details page.

This page shows the details of the selected access point including the hardware, operating system software, and boot version details.

General Tab

The following parameters are not displayed for ODM access point under General parameters:

• AP Mode

• AP Sub Mode

This table describes the general AP parameters.

Table 5-2   General Tab Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Location	User-definable location name for the access point. You can enter up to 254 characters.
AP MAC Address	MAC address of the access point.
Base Radio MAC	MAC address of the 802.11a/b/g/n radio.
Admin Status	Administration state of the access point.
AP Mode	Access point mode of operation. The options are as follows:
	Note The Cisco OEAP 600 Series access point uses local mode and these settings cannot be altered. Monitor mode, Sniffer mode, Rogue detector mode, Bridge mode, and SE- Connect modes are not supported on the 600 OEAP series.
	• Local—Default option.
	• FlexConnect—AP mode that is used for 1130AG, 1140, 1240AG, 1250, and AP801 access points.
	• Monitor—Monitor-only mode.
	• Rogue Detector—AP mode that monitors the rogue APs; the mode does not transmit or contain rogue APs.
	• Sniffer—AP mode that starts sniffing the wireless network on a given channel. It captures and forwards all the packets from the clients on that channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). It will include information on timestamps, signal strength, packet size and so on.
	See the Sniffer Feature topic for more details.
	• Bridge—AP mode that is a bridge if you are connecting a root AP.
	Note This option is displayed only if the AP is bridge capable.
	Note If the AP mode is set to "Bridge" and the AP is not REAP capable, an error is displayed.
	• SE-Connect—AP mode that is SE-Connect if you want the access point to perform spectrum intelligence. This field does not appear for Cisco Aironet 1520 and 1550 Series access points.
	Note Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.
	Note When an access point is configured in SE-Connect mode, the access point reboots and rejoins the controller. Access points configured in this mode will not serve clients.
	Note To configure an access point for wIPS, you must set the AP mode to one of the following from the AP Mode drop-down list: Local, FlexConnect, or Monitor.

Table 5-2   General Tab Parameters

Parameter	Description
AP Sub Mode	Access Point submode. The available options are as follows: • WIPS—The AP is in local, FlexConnect, or monitor mode and the wIPS submode is configured on the access point. • None—The AP is in local/FlexConnect mode and WIPS submode is not configured on the AP. **Note** wIPS ELM is not supported on 1130 and 1240 access points.
Operational Status	Operational status of the access point that comes up as either registered (REG) or not registered (DEREG) automatically by the Cisco WLC.
Port Number	Access point that is connected to this Cisco WLC port.
Network Spectrum Interface Key	32-digit Network Spectrum Interface (NSI) key. The NSI key is required to configure spectrum expert mode. **Note** This parameter is shown only for CleanAir capable access points for only Local, FlexConnect, and SE-Connected mode.
Venue Group	Drop-down list from which you can choose a Hotspot group that groups similar Hotspot venues. The following options are available: • Unspecified • Assembly • Business • Educational • Factory and Industrial • Institutional • Mercantile • Residential • Storage • Utility and Misc • Vehicular • Outdoor
Venue Type	Drop-down list from which you can choose the type of venue based on the Venue Group that you choose.
Venue Name	Venue name that you can provide for this access point. This name is associated with the basic service set (BSS). This name is used in cases where the SSID does not provide enough information about the venue. The venue name is case sensitive and can be up to 252 alphanumeric characters.
Language	Language used at the venue. ISO-639 encoded string defining the language used at the venue. This string is a three-character language code. For example, you can enter ENG for English.

Table 5-2   General Tab Parameters

Parameter	Description
Network Spectrum Interface (NSI) Key	When an access point in SE-Connect mode joins a controller, it sends a Spectrum Capabilities notification message, and the controller responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the controller for use in NSI authentication. The controller generates one key per access point, which the access point stores until it is rebooted.
The following parameters are applicable to Cisco 1570 Series Access Points	
Internal Temperature	The Internal Temperature of the AP is displayed in both Celsius and Fahrenheit.
Temperature State	The Temperature State is shown to be in one of three states: GREEN, YELLOW, or RED. The GREEN state indicates that the AP is functioning normally and the internal temperature is at an optimal operating temperature; the YELLOW state indicates that the AP state is in transition to either GREEN or RED state; if the AP is in RED state, it means that the internal temperature of the AP has increased and the number of antennas that are used for transmission will be reduced.
Heater Status	Not applicable to 1570 APs.
PoE Out State	The PoE Out State shows the status of the Power over Ethernet output port from the AP. The PoE Out State can be in OFF or ON state depending on the input power source for the AP.

The following parameters are not displayed for Cisco OEAP 600 Series access point:

- Predownload Status
- Predownloaded Version
- Predownloaded Next Retry Time
- Predownload Retry Count
- All the predownload parameters
- IOS Version
- Mini IOS Version

This table describes the GPS Location parameters. GPS parameters do not appear if the access point does not have a GPS module or the GPS information is invalid.

Table 5-3   GPS Location Parameters

Parameter	Description
GPS Present	GPS module that is installed on the access point or not.
Latitude	Latitude information of the access point in the GPS data received.
Longitude	Longitude information of the access point in the GPS data received.
Altitude	Altitude information of the access point in the GPS data received.
GPS Location Age	Time when the GPS data was collected.

This table describes the Cable Modem statistics. The Cable Modem statistics are updated every 5 minutes after the AP is associated with the WLC. The Cable Modem statistics are applicable for Cisco 1572C (internal or external antenna cable modem) access points in local or bridge/Flex-bridge modes.

Table 5-4   Cable Modem Statistics

Parameter	Description
Cable Modem Statistics	Information about the following is shown: • AP Name • AP MAC Address • CM MAC Address • CM Software Version • Ethernet Speed • Ethernet Status • Docsis Registration Status • CM Serial Number • CM Mask
US Channel Status	Information about the following is shown: • Channel ID • Power Level • Center Frequency • Carrier to Noise Ratio
DS Channel Status	Information about the following is shown: • Channel ID • Power Level • Center Frequency

This table describes the version parameters.

Table 5-5   Version Parameters

Parameter	Description
Primary Software Version	Primary software version.
Backup Software Version	Version of the backup software on this access point.
Predownload Status	Predownload status on this access point.
Predownloaded Version	Version of the software that is being predownloaded.
Predownload Next Retry time	Time duration after which this access point will try to perform a predownload operation.

Table 5-5   ***Version Parameters***

Parameter	Description
Predownload Retry Count	Number of times this access point has tried to perform the predownload operation.
Boot Version	Boot ROM versions.
IOS Version	Cisco IOS software version.
Mini IOS Version	Mini-IOS software version.
GPS Location	GPS parameters do not appear if the access point does not have a GPS module or the GPS information is invalid.
GPS Present	GPS module that is installed on the access point or not.
Latitude	Latitude information of the access point in the GPS data received.
Longitude	Longitude information of the access point in the GPS data received.
Altitude	Altitude information of the access point in the GPS data received.
GPS Location Age	Time when the GPS data was collected.

This table describes the IP config parameters.

Table 5-6   ***IP Config Parameters***

Parameter	Description
CAPWAP Preferred Mode	Displays the current CAPWAP Preferred mode of the AP. It can be: • IP Config (Global)— Configured at Controller > General. • IP Config (AP Group Config)—Configured at WLAN > Advanced > AP Groups > General Tab.
DHCPv6 Address	Displays the DHCP IPv6 address.

Table 5-6   *IP Config Parameters*

Parameter	Description
Static IP (IPv4/IPv6)	Check box to enable configuration of the AP using static IP address. From Release 8.0, IPv4 and IPv6 are supported.
Static IP (IPv4/IPv6)	Static IP address of the access point.
	When an access point boots up, it tries to determine if its static IP address is configured or not. If the access point has been configured with a static IP address that is not valid on the network, the access point cannot join the controller and cannot communicate with the rest of the network. In such a scenario, the only way to recover that access point is to manually open the access point door and connect a serial console for configuration purpose.
	The access point can be configured in such a way that, even if its static IP address is not valid on the network, it initiates a DHCP process to get a new IP address and use it for communication. This configuration enables the access point to join the controllers on the network.
	Note An access point cannot discover the controller using domain name system (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs.
	Options for this parameter are as follows:
	• Unselected—When this check box is not selected, the static IP address is disabled and the access point initiates a DHCP process when it boots up to procure the IP address.
	• Checked—When this check box is selected, you can set the following:
	– The static IPv4/IPv6 address of the access point.
	– The subnet mask/ prefix length assigned to the access point IPv4/IPv6 address.
	– The IPv4/IPv6 gateway of the access point.
	Click **Apply** to commit your changes. The access point reboots and rejoins the controller, and the static IP address that you specified in is sent to the access point. You can now configure the DNS server IP address and domain name. To do so, follow these steps:
	– In the DNS IP Address text box, enter the IPv4/IPv6address of the DNS server.
	– In the Domain Name text box, enter the name of the domain to which the access point belongs.
	Click **Apply** to commit your changes.

This table describes the time statistics.

Table 5-7   Time Statistics Parameters

Parameter	Description
UP Time	Amount of time that the access point has been powered up.
Controller Associated Time	Amount of time that the access point has been associated with the controller.
Controller Associated Latency	Amount of time that the access point took to associate with the controller.

- Click **Reset AP Now** to reset the access point.
- Click **Clear All Config** to reset the access point parameters to the factory defaults.
- Click **Clear Config Except Static IP** to reset the access point parameters to the factory defaults but retains the static IP address information.

Credentials Tab

Note   The Credentials Tab is not displayed for ODM access points.

This table describes the credentials parameters.

Table 5-8   Credentials Tab Parameters

Parameter	Description
Over-ride Global credentials	Access point that is prevented from inheriting the global username, password, and enable password from the controller. The default value is unselected.
Username	Unique username for this access point.
Password	Unique password for this access point.
Enable Password	Unique enable password for this access point.

This table describes the controller configuration parameters.

Table 5-9   802.11X Supplicant Credentials Parameters

Parameter	Description
Over-ride Global credentials	Access point that is prevented from inheriting the global authentication username and password from the controller. The default value is unselected.
Username	Unique username for this access point.

Table 5-9   802.11X Supplicant Credentials Parameters

Parameter	Description
Password	Unique password for this access point.
	Note You must enter a strong password. Strong passwords have the following characteristics:
	• They are at least eight characters long.
	• They contain a combination of uppercase and lowercase letters, numbers, and symbols.
	• They are not words in any language.
Confirm Password	Unique password that you can reenter for this access point.

Interfaces Tab

Note   To enable or disable CDP either on an Ethernet or radio interface, you should enable the global CDP for that particular access point. See Global Configuration for more information.

Note   CDP over radio interface is applicable only for mesh APs.

Note   The CDP state and CDP configuration are not displayed for the Cisco OEAP 600 Series access point under the Ethernet Interfaces parameters.

This table describes the ethernet interface parameters.

Table 5-10   Ethernet Interface Parameters

Parameter	Description
CDP Configuration	
Ethernet Interface#	Ethernet interface number.
CDP State	Current configured state of CDP on all or a specific Ethernet interface. The status could be enabled or disabled.
	Note You can enable or disable CDP on all or a specific Ethernet interface by choosing **WIRELESS** > **Access points** > **Global Configuration** and select **CDP State** check box over a particular Ethernet interface.
Interface	CDP interface name.
Operational Status	Status of the interface.
Tx Unicast Packets	Number of unicast packets transmitted.
Rx Unicast Packets	Number of unicast packets received.

Table 5-10   Ethernet Interface Parameters

Parameter	Description
Tx Non-Unicast Packets	Number of nonunicast packets transmitted.
Rx Non-Unicast Packets	Number of nonunicast packets received.

Click an interface name to view its properties.

This table describes the interface parameters.

Table 5-11   Interface Properties Parameters

Parameter Name	Description
AP Name	Name of the access point.
Link speed	Speed of the interface in Mbps.
RX Bytes	Total number of bytes in the error-free packets received on the interface.
RX Unicast Packets	Total number of unicast packets received on the interface.
RX Non-Unicast Packets	Total number of nonunicast or multicast packets received on the interface.
Input CRC	Total number of CRC error in packets received on the interface.
Input Errors	Sum of all errors in the packets while receiving on the interface.
Input Overrun	Number of times the receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the receiver's capability to handle the data.
Input Resource	Total number of resource errors in packets received on the interface.
Runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
Throttle	Total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.
Output Collision	Total number of packets retransmitted due to an Ethernet collision.
Output Resource	Resource errors in packets transmitted on the interface.
Output Errors	Errors that prevented the final transmission of packets out of the interface.
Operational Status	Operational state of the physical Ethernet interface on the AP.

Table 5-11   Interface Properties Parameters

Parameter Name	Description
Duplex	Interface's duplex mode.
TX Bytes	Number of bytes in the error-free packets transmitted on the interface.
TX Unicast Packets	Total number of unicast packets transmitted on the interface.
TX Non-Unicast Packets	Total number of nonunicast or multicast packets transmitted on the interface.
Input Aborts	Total number of packets aborted while receiving on the interface.
Input Frames	Total number of packets received incorrectly that had a CRC error and a noninteger number of octets on the interface.
Input Drops	Total number of packets dropped while receiving on the interface because the queue was full.
Unknown Protocol	Total number of packets discarded on the interface due to an unknown protocol.
Giants	Number of packets that are discarded because they exceeded the medium's maximum packet size.
Interface Resets	Number of times that an interface has been completely reset.
Output No Buffer	Total number of packets discarded because there was no buffer space.
Output Underrun	Number of times the transmitter has been running faster than the router can handle.
Output Total Drops	Total number of packets dropped while transmitting from the interface because the queue was full.

This table describes the radio interface parameters.

Table 5-12   Radio Interface Parameters

Parameter	Description
Number of Radio interfaces	Number of radio interfaces.
CDP Configuration	
Radio Slot#	Slot where the radio is installed.
CDP State	Current configured state of CDP on the radio slot. The status could be enabled or disabled.
	Note You can enable or disable CDP on all or a specific access point by choosing **WIRELESS > Access points > Global Configuration** and selecting the **CDP State** check box over a particular radio interface.

Table 5-12   Radio Interface Parameters

Parameter	Description
Radio Interface Type	Cisco Radio type. The value is either 802.11a/n/ac, 802.11b/g/n, or 802.11a/b/g/n. 802.11a/b/g/n appears if you have the monitor module for 3600 access points.
Module Type	Access Point module type.
Sub Band	Radio sub band, if it is active. The value is either 4.9 GHz or 5.8 GHz.
Admin Status	Cisco Radio interface status.
Oper Status	Cisco Radio operational status.
CleanAir Admin Status	CleanAir administration status.
CleanAir Oper Status	CleanAir operational status.
Regulatory Domain	Regulatory domain that is supported or unsupported.

High Availability Tab

The high availability feature is used to help an AP move over to a controller when the current controller fails. The backup and secondary are the fourth and fifth in the order of controllers if primary, secondary, and tertiary controllers are configured under the AP. If the primary, secondary, and tertiary controllers are not configured, then the AP will use the backup primary if the current controller fails.

Note   If the AP supports IPv6 then it can discover a WLC over IPv6 CAPWAP tunnel.

Note   When the Cisco OEAP 600 Series access point joins the controller, the high availability settings have only the IP address that have been entered in the local UI of the OEAP 600 Series from the controller.

This table describes the high availability parameters.

Table 5-13   High Availability Parameters

Parameter	Description
Primary Controller	Name and management IP address of the primary controller. From Release 8.0, IPv4 and IPv6 are supported.
Secondary Controller	Name and management IP address of the secondary controller. From Release 8.0, IPv4 and IPv6 are supported.

Table 5-13   *High Availability Parameters*

Parameter	Description
Tertiary Controller	Name and management IP address of the tertiary controller. From Release 8.0, IPv4 and IPv6 are supported.
AP Failover Priority	Priority for the access point: • Low—Assigns the access point to the level 1 priority, which is the lowest priority level. This is the default value. • Medium—Assigns the access point to the level 2 priority. • High—Assigns the access point to the level 3 priority. • Critical—Assigns the access point to the level 4 priority, which is the highest priority level.

Inventory Tab

This table describes the inventory parameters.

Table 5-14   *Inventory Tab Parameters*

Parameter	Description
Product ID	Model of the access point.
Version ID	Version of the access point.
Serial Number	Serial number of the access point; for example, FTX0916T134.
Entity Name	Entity name of the access point.
Entity Description	Entity description of the access point.
Certificate Type	Certificate type as either Self Signed or Manufacture Installed.
FlexConnect Mode Supported	Whether the access point can be configured as a remote edge lightweight access point. The values are Yes or No. FlexConnect Mode is supported on the 1130AG, 1240AG, and 1250 access points. **Note** By default, a VLAN is not enabled on the FlexConnect. After it is enabled, FlexConnect inherits the VLAN name (interface name) and VLAN ID associated to WLANs. This configuration is saved in the access point and received after the successful join response. By default, no VLAN is set as a native VLAN. There must be one native VLAN configured per REAP in a VLAN-enabled domain. Otherwise, REAP cannot send packets to or receive packets from the controller. When the client gets assigned a VLAN from the RADIUS server for the client, that VLAN is associated to the local switched WLAN. **Note** Black list—FlexConnect supports the first 128 entries in the list in the standalone mode.

Mesh Tab

Note   This tab appears if you set the AP Mode on the General Tab to Bridge.

This table describes the mesh parameters.

Table 5-15   Mesh Tab Parameters

Parameter	Description
AP Role	Root AP or Mesh AP.
	Root APs have a wired CAPWAP (Control and Provisioning of Wireless Access Points) protocol connection back to a controller. This connection uses the backhaul wireless interface to communicate to neighboring Mesh APs. Root APs are parent nodes to any bridging or mesh network and connect a bridge or mesh network to the wired network. You can have only one Root AP for any bridged or mesh network.
	Mesh APs have no wired connection to a controller. They can be completely wireless supporting clients, communicating to other Mesh APs and a Root AP to get access to the network, or they can be wired and serve as a bridge to a remote wired network.
Bridge Type	(Display Only Field) Whether the access point is an indoor or outdoor access point.
Bridge Group Name	Bridge group name.
	Use bridge group names to logically group the access points and to avoid two networks on the same channel from communicating with each other.
	Note For the access points to communicate with each other, they must have the same bridge group name.
Ethernet Bridging	Ethernet bridging on the access point.
	If the AP Mode is Root AP, Ethernet bridging is enabled by default.
	If the AP Mode is Mesh AP, Ethernet bridging is disabled by default.
	Enable Ethernet bridging on a Mesh AP if you want to do one of the following:
	• Use the mesh nodes as bridges.
	• Connect an Ethernet device on the Mesh AP using its Ethernet port.
	Note When you enable Ethernet Bridging and click **Apply**, the Ethernet Bridging Parameters area appears and lists the four Ethernet ports of the mesh access point.
Backhaul Interface	(Display Only Field) Backhaul interface (802.11a, 802.11b, 802.11g, or 802.11n).

Table 5-15   Mesh Tab Parameters

Parameter	Description
Bridge Data Rate (Mbps)	Rate at which data is shared between the access points. The drop-down list displays the data rates depending on the Backhaul Interface set.
	The correct range of values depend on the backhaul interfaces used by the access points.
	The data rates (Mbps) are as follows:
	• 802.11a: auto, 6, 9, 12, 18, 24, 36, 48, 54
	Note In previous software releases, the default value for bridge data rate for 802.11a was 24 Mbps. In controller release 6.0, the default value for the bridge data rate is auto. If you configured the default bridge data rate value (24 Mbps) in a previous controller software release, the bridge data rate is configured with the new default value (auto) when you upgrade to controller software release 6.0. However, if you configured a nondefault value (for example, 18 Mbps) in a previous controller software release, that configuration setting is preserved when you upgrade to software release 6.0. When the bridge data rate is set to auto, the mesh backhaul chooses the highest rate where the next higher rate cannot be used due to unsuitable conditions for that specific rate (and not because of conditions that affect all rates).
	• 802.11b: 1, 2, 5.5, 11
	• 802.11g: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54
Ethernet Link Status	Status of the Ethernet (LAP1510) or Gigabit Ethernet (LAP1522) links. For each link, the status can be Up, Dn, or Na.
Heater Status	Status of the heater.
Internal Temperature	Internal temperature of the access point in Fahrenheit and Celsius.

Note The following parameters appear when you enable Ethernet Bridging and click **Apply**.

This table describes the Ethernet bridging parameters.

Table 5-16   Ethernet Bridging Parameters

Parameter	Description
Interface Name	Name of the interface. Click the interface name to open the VLAN Mappings for Mesh Access Points page.
	To configure access mode on a Mesh access point, click the **gigabitEthernet1** interface.
	To configure trunk mode on a Root or Mesh access point, click the **gigabitEthernet0** interface.
Oper Status	Operational status of the interface.

Table 5-16   Ethernet Bridging Parameters

Parameter	Description
Mode	Mode of the interface: Normal, Access, or Trunk.
VLAN ID	VLAN ID of the interface.

FlexConnect Tab

Note   This tab appears if you set the AP Mode on the General Tab to FlexConnect.

This table describes the FlexConnect parameters.

Table 5-17   FlexConnect Parameters

Parameter	Description
VLAN Support	Check box to configure the native VLAN ID and the VLAN mappings. **Note** After you enable VLAN support, click **Apply** to activate the VLAN Mappings button.
Inheritance Level	Shows the status of the VLAN Support configuration. If Native VLAN on AP is overridden, then this is shown as Group Specific.
Make VLAN AP Specific/Remove VLAN AP Specific	Drop-down list to configure VLAN support for the FlexConnect AP. When the override flag at the FlexConnect group is disabled, this additional inheritance level configuration is available for the FlexConnect AP. If you choose "Make VLAN AP Specific," then the VLAN support, Native VLAN ID, and WLAN-VLAN mappings are made specific to this AP and not to the FlexConnect group.
Native VLAN ID	VLAN ID number.
VLAN Mappings	VLAN mappings for the locally switched WLANs. Click the **VLAN Mappings** button. You can also view VLAN-ACL mappings on the AP via FlexConnect groups.
FlexConnect Group Name	Name of the group if the access point belongs to a FlexConnect group. See the FlexConnect Groups page for more information about FlexConnect groups.
PreAuthentication Access Control Lists	
External WebAuthentication ACLs	ACLs for external web authentication. Click the **External WebAuthentication ACLs** link to view and configure the ACL mappings and web policy ACLs.
Local Split ACLs	ACLs for the local split WLANs. Click the **Local Split ACLs** link to view and configure the local split ACLs of the REAP groups. These ACLs locally switch traffic in centrally switched WLANs.
Central DHCP Processing	Central DHCP processing parameters. Click the Central DHCP Processing link to view the WLAN DHCP mappings and configure WLAN DHCP parameters such as Central DHCP, Override DNS, and NAT/PAT. Click **Add** to create a new WLAN DHCP mapping.

Table 5-17   FlexConnect Parameters

Parameter	Description
OfficeExtend AP	
Note	Only Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 Series Controller with a WPlus license can be configured to operate as OfficeExtend access points. For more information, see the OfficeExtend Access Points topic.
Enable OfficeExtend AP	OfficeExtend mode for this access point. The default value is enabled. **Note** Unselecting this check box disables OfficeExtend mode for this access point. It does not undo all the configuration settings on the access point.
Enable Least Latency Controller Join	Access point to choose the controller with the least latency when joining. The default value is disabled. When you enable this feature, the access point calculates the time between the discovery request and the discovery response and joins the Cisco 5500 Series Controller that responds first.
Reset Personal SSID	Access point's personal SSID that you can clear. **Note** If you want to clear the access point's configuration and return it to the default settings, enter the **clear ap config** *Cisco_AP* command on the controller CLI.

Mesh Tab

Note   This tab appears only for Mesh APs.

This table describes the mesh parameters.

Table 5-18   Mesh Parameters

Parameter	Description
AP Role	Drop-down list from which you can choose a Root AP or Mesh AP.
Bridge Type	Type of bridge that can Indoor or Outdoor.
Bridge Group Name	Bridge group names (BGNs) that control the association of mesh access points. BGNs can logically group radios to avoid two networks on the same channel from communicating with each other. The setting is also useful if you have more than one RAP in your network in the same sector (area). The BGN can be a string of up to 10 characters.
Ethernet Bridging	Check box that you enable to configure Ethernet bridging. For security reasons, the Ethernet port on all MAPs is disabled by default. It can be enabled only by configuring Ethernet bridging on the root and its respective MAP. You must enable Ethernet bridging in the following scenarios: • When you want to use the mesh nodes as bridges. • When you want to connect any Ethernet device such as a video camera on the MAP using its Ethernet port. This is the first step to enable VLAN tagging.

Table 5-18   Mesh Parameters

Parameter	Description
Backhaul Interface	Backhaul interface on which the access point operates. Backhaul is used to create only the wireless connection between the access points. The default backhaul interface is 802.11a or 802.11a/n/ac depending upon the access point.
Bridge Data Rate	Drop-down list from which you can choose the data rate of the bridge. The rate selection is important for effective use of the available RF spectrum. The rate can also affect the throughput of client devices.
Ethernet Link Status	Status of the Ethernet link.
Heater Status	Heater status of the access point.
Internal Temperature	Internal temperature of the access point.

Advanced Tab

The following parameters are not displayed for the Cisco OEAP 600 series access point:

- Cisco Discovery Protocol
- Rogue Detection
- Telnet
- SSH

This table describes the advanced parameters.

Table 5-19   Advanced Tab Parameters

Parameter	Description
Regulatory Domains	Regulatory domain of the AP.
Country Code	Country code. See the Country topic for information on configuring the country code.
Cisco Discovery Protocol	Cisco Discovery Protocol that you can enable or disable. The default is unselected. **Note** If CDP is disabled at the controller level, a message "Controller CDP Disabled" appears.
AP Group Name	AP Group's VLANs that you have created. To associate an AP group VLAN with an access point, follow these steps: **1.** Select an AP group VLAN from the drop-down list. **2.** Click **Apply**. For more information on creating a new AP group and mapping it to an interface, see the AP Groups page.
Statistics Timer	Time in seconds that the access point sends its 802.11 statistics to the Cisco WLC.

Table 5-19   *Advanced Tab Parameters*

Parameter	Description
Data Encryption	Datagram Transport Layer Security (DTLS) data encryption that you can enable or disable. The default is unselected.
	Cisco 5500 Series Wireless Controllers enable you to encrypt CAPWAP control packets (and optionally, CAPWAP data packets) that are sent between the access point and the controller using DTLS. DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS. CAPWAP control packets are management packets exchanged between a controller and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data). If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.
	Note If an access point with data encryption enabled tries to join any other controller, the access point joins the controller, but data packets are sent unencrypted.
	DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points. Most access points are deployed in a secure network within a company building, so data encryption is not necessary. The traffic between an OfficeExtend access point and the controller travels through an unsecure public network, so data encryption is more important for these access points. When data encryption is enabled, traffic is encrypted at the access point before it is sent to the controller and at the controller before it is sent to the client.
	Note Encryption limits throughput at both the controller and the access point, and maximum throughput is desired for most enterprise networks.
	The availability of data DTLS for the 7.1 release is as follows:
	• The Cisco 5500 Series Controller will be available with two licenses options. One that allows data DTLS without any license requirements and another image requiring a license to use data DTLS. The images for the DTLS and licensed DTLS images are as follows:
	– Licensed DTLS—AS_5500_LDPE_x_x_x_x.aes
	– Non licensed DTLS—AS_5500_x_x_x_x.aes
	• Cisco 7500, 2500, WiSM2, WLC2—These platforms by default will not contain DTLS. To turn on data DTLS, a license must be installed. That is, these platforms will have a single image with data DTLS turned off. To use data DTLS you must have a license.
	Note If your controller does not have data DTLS license and if the access point associated with the controller has DTLS enabled, the data path will be unencrypted.
	The following are some of the guidelines when upgrading to or from a DTLS image:
	• You cannot install a regular image (DTLS enabled) once a non-DTLS image is installed.
	• You can upgrade from one licensed DTLS image to another licensed DTLS image.
	• You can upgrade from a regular image (DTLS) to a licensed DTLS image in a two step process.
	• You cannot upgrade from a licensed DTLS image to any regular image.
Rogue Detection	Rogue detection for individual access points that you can enable or disable. Rogue detection is enabled by default for all access points joined to the controller (except for OfficeExtend access points). The default is unselected.

Table 5-19   Advanced Tab Parameters

Parameter	Description
AP Sub Mode	AP submode that displays *wIPS* if the access point is in Monitor mode (from the **AP Mode** drop-down list on the General Tab) and the wIPS submode is configured on the access point or *None* if the access point is in local/FlexConnect modes and wIPS submode is not configured. **Note** wIPS ELM is not supported on 1130 and 1240 access points.
Telnet	Telnet or SSH connectivity on this access point. The default is unselected.
SSH	These protocols make debugging the access point easier, especially when the access point is unable to connect to the controller.
TCP Adjust MSS	Enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router on a per AP basis. From Release 8.0, the controller supports IPv6. Use the following Global TCP Adjust MSS values for: • IPv4—Specify a value between 536 and 1363. • IPv6—Specify a value between 1220 and 1331. **Note** Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP
UDP Lite	Displays the per AP UDP lite status. **Note** The UDP Lite field is displayed only for APs that are associated using CAPWAP v6. This field is not displayed for APs associated using IPv4 address.
Disable LAN Ports	Parameter that makes the AP work only as a wireless AP. **Note** This option is applicable only for Cisco 600 Series OfficeExtend Access Points.
Disable Personal SSID	Parameter that disallows users from setting up personal SSIDs. **Note** This option is applicable only for Cisco 600 Series OfficeExtend Access Points.
LED State	Parameter to enable or disable the LED state of the AP to be shown.
LED Flash State	• Click the LED flash duration for the AP option and enter the duration range from 1 to 3600 seconds • Click the **Indefinite** option to configure the LED to flash indefinitely • Click the **Disable** option to stop flashing the LED
Link Latency	
Note The Link Latency parameters are not displayed for ODM access points.	
Enable Link Latency	Link latency for this access point. Enable link latency to measure the link between an access point and the controller. This feature can be used with all access points joined to the controller but is especially useful for FlexConnect access points (in connected mode) and OfficeExtend access points, for which the link could be a slow or unreliable WAN connection. **Note** FlexConnect access points in standalone mode are not supported.
Current (mSec)	Current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
Minimum (mSec)	Minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back since link latency has been enabled or reset.

Table 5-19   Advanced Tab Parameters

Parameter	Description
Maximum (mSec)	Maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back since link latency has been enabled or reset.
Reset Link Latency	Link latency statistics on the controller for this access point.

AP Image Download

Note   The 1120, 1230, and 1310 access points do not support predownloading of images.

Parameter	Description
Perform a primary image pre-download for this AP	Primary image predownload. Click **Download Primary** to perform a primary image predownload for this access point. An alert box displays the version that would be downloaded when the access point boots. Click **OK** to continue.
Perform an interchange of both the images on this AP	Interchange of images. Click **Interchange Image** to change the images on this access point. A dialog box prompts you to confirm if you want to interchange the images. Click **OK** to continue.
Perform a backup image pre-download for this AP	Backup image predownload. Click **Download Backup** to predownload a backup image for this access point. A pop-up window displays the version that would be downloaded when the access point boots. Click **OK** to continue.

Power Over Ethernet Settings

Note   The Power Over Ethernet Settings parameters are not displayed for Cisco OEAP 600 Series access points.

Parameter	Description
PoE Status	Status that applies only to 1250 series access points that are powered using PoE. This field shows the power level at which the access point is operating: High (20 W), Medium (16.8 W), or Medium (15.4 W). This field is not configurable. The controller automatically detects the access point's power source and displays the power level here. **Note** There are two other ways to tell if the access point is operating at a lower power level. First, the "Due to low PoE, radio is transmitting at degraded power" message appears under the Tx Power Level Assignment section on the Configuring 802.11a/n APs page. Second, the "PoE Status: degraded operation" message appears in the controller's trap log on the Trap Logs page.
Pre-Standard State	Whether the access point is being powered by a high-power Cisco switch. Unselect the check box if power is being provided by a power injector. This option is disabled by default.
Power Injector State	Whether the attached switch supports intelligent power management (IPM) and a power injector is being used. If the attached switch supports IPM, you do not need to select this check box.
Power Injector Selection	One of the following options: • Installed—Select the check box if you want the access point to examine and remember the MAC address of the currently connected switch port (this selection assumes that a power injector is connected). If you want to configure the switch MAC address, enter the MAC address in the Injector Switch MAC address text box. • Override—Select the check box to enable the access point to operate in high-power mode without first verifying a matching MAC address.

Table 5-19   Advanced Tab Parameters

Parameter	Description
Injector Switch MAC Address	MAC address of the connected switch port.
AP Core Dump Settings	
Note The File Compression parameter is not displayed for ODM access points.	
AP Core Dump	Upload the access point core dump. The default is enabled.
TFTP Server IP	IP address of the TFTP server. From release 8.0, the TFTP server supports IPv6 address too.
File name	Access point core dump file (for example, dump.log).
File Compression	File compression of the access point core dump file. When you enable this option, the file is saved with a .gz extension (for example, dump.log.gz). This file can be opened with WinZip. The default is disabled.
AP Retransmit Config Parameters	
AP Retransmit Count	Number of times that you want the access point to retransmit the request to the controller and vice versa. The range is from 3 to 8.
AP Retransmit Interval	Time duration between retransmission of requests. The range is from 2 to 5.
VLAN Tagging Settings	
VLAN Tagging	VLAN tagging of the CAPWAP packets that you can enable or disable.
Trunk VLAN ID	ID of the trunk VLAN. If the access point is unable to route traffic through the specified trunk VLAN, it untags the packets and reassociates with the controller. The controller sends a trap to a trap server such as the Cisco PI, which indicates the failure of the trunk VLAN. If the trunk VLAN ID is zero, the access point untags the CAPWAP packets.
VLAN Tag Status	Whether the access point tags or untags the CAPWAP packets.

Click **Apply** to send data to the controller, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Sniffer Feature

When the sniffer feature is enabled on an access point, the access point functions as a sniffer and captures and forwards all the packets on a particular channel to a remote machine that runs AirMagnet Enterprise Analyzer, Airopeek, or Wireshark. These packets contain information on timestamps, signal strengths, packet sizes and so on.

Note   You can enable the sniffer feature only if you are running Airopeek or Wireshark (third-party network analyzer software that supports decoding of data packets).

> ✎
>
> **Note**   You must disable IP-MAC address binding in order to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller, or a controller network module running software release 6.0. To disable IP-MAC address binding, enter the **config network ip-mac-binding disable** command from the controller CLI.

> ✎
>
> **Note**   You must enable WLAN 1 to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller, or a controller network module running software release 6.0. If WLAN 1 is disabled, the access point cannot send packets.

Before using the sniffer feature, you must configure an access point in sniffer mode at the remote site. See the *Cisco Wireless LAN Controller Configuration Guide* for installation information for AirMagnet Enterprise Analyzer, Airopeek, and Wireshark packet analyzers for IEEE 802.11 wireless LANs.

Traffic Stream Metrics Collection

Choose **MONITOR > Wireless > Clients** and then click **802aTSM** or **802b/gTSM** to navigate to the Traffic Stream Metrics page.

Traffic stream metrics involves collecting of uplink statistics and downlink statistics between an AP and a CCX v4 client and then propagating these statistics periodically back to the controller. If the client is not CCXv4 compliant, then only downlink statistics are captured.

Traffic stream metrics collection can be configured by the user for each interface band (for example, all 802.11a radios). The controller also saves this option in flash memory so that it persists across reboots. Once an AP receives this message, it enables traffic metrics collection feature on the specified interface type.

Every 5 seconds, the AP gets a measurement report for both the uplink (client side) and downlink (local side) measurements. The aggregation of 5-second reports and preparation of 90-second reports is done at the AP. Every 90 seconds, the AP prepares an IAPP data packet and sends it to the controller for further processing. The controller stores the data in its structures and then provides "usmdB" access APIs to the CLI module and the WCS for displaying it on the UI.

Four variables are affected by the WLAN that can affect audio quality: packet latency, packet jitter, packet loss and roaming time. You can isolate the problem of bad voice quality by studying these variables. The traffic stream metrics feature addresses the voice quality issue by providing an administrator with statistics for each of these four variables.

OfficeExtend Access Points

Currently, Cisco Aironet 1130, 1140, 3502I, 600 series access points that are joined to a Cisco 5500 Series Controller can be configured to operate as OfficeExtend access points.

An OfficeExtend access point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The experience of the teleworker at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Guidelines and Limitations

1. OfficeExtend access points are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), enabling an entire group of computers to be represented by a single IP address. In controller software release 6.0 or later releases, only one OfficeExtend access point can be deployed behind a single NAT device.

2. Rogue detection is disabled when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point by selecting the Rogue Detection check box on the All APs Details for (Advanced) page. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

3. DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point by selecting the Data Encryption check box on the All APs Details for (Advanced) page.

4. Telnet and SSH access are disabled when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point by selecting the Telnet or SSH check box on the All APs Details for (Advanced) page.

5. Link latency is enabled when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point by selecting the Enable Link Latency check box on the All APs Details for (Advanced) page.

6. The Cisco OEAP 600 Series access point supports a maximum of two WLANs and one remote LAN. If you have configured more than two WLANs and one remote LAN, you can assign the Cisco OEAP 600 Series access point to an AP Group. The support for two WLANs and one remote LAN still applies to the AP Group if the Cisco OEAP 600 Series is in the default group. The WLAN/remote LAN IDs must be less than 8.

7. Only four clients can connect to an Cisco OEAP 600 Series access point through a remote LAN port. This number does not affect the 15-client limit imposed for the Cisco WLC WLANs. The remote LAN client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices will be able to connect until one of the devices is idle for more than one minute.

8. CAC is not supported on the Cisco OEAP 600 Series access points.

9. Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the Cisco WLC.

controller release 7.1 and later supports OEAP 600 series access points on Cisco 5508, Catalyst 6500 Series Wireless Services Module (WISM-2), and 2500 Series Controllers. Unlike the 1130 and 1140 series access points which required configuration for FlexConnect and setting the sub-mode of the access point to OEAP, the 600 series uses local mode and these settings cannot be altered.

The following access point modes are not supported on the Cisco OEAP 600 Series access points:

- Monitor mode
- FlexConnect mode
- Sniffer mode
- Rogue Detector Bridge mode
- SE-Connect mode

VLAN Mappings for FlexConnect Access Points

Choose **WIRELESS > Access Points > All APs**, click the AP name of a FlexConnect access point, click the **FlexConnect** tab, and then click **VLAN Mapping** to navigate to the VLAN Mappings page. This page enables you to assign a VLAN ID to the FlexConnect access point and configure VLAN mappings for the locally switched WLANs. You can also view VLAN-ACL mappings on the AP via the FlexConnect group.

This table describes the VLAN mapping parameters.

Table 5-20   VLAN Mapping Parameters

Parameter	Description
AP Name	Name of the access point.
Base Radio MAC	MAC address of the 802.11a/b/g/n radio.
WLAN VLAN Mapping	
Drop-down list	To make the WLAN-VLAN mapping as either specific the FlexConnect AP or to remove the configuration.
WLAN ID	WLAN ID number.
SSID	Name of the WLAN.
VLAN ID	Number of the VLAN from which the clients receive an IP address when doing local switching.
NAT-PAT	Status of Network Address Translation and Port Address Translation on the locally switched WLANs.
Inheritance	Shows the VLAN support inheritance status.
Centrally Switched WLANs	
WLAN ID	WLAN ID to which this is mapped to.
SSID	Service Set Identifier of the WLAN.
VLANID	VLAN ID of the WLAN.
AP	Access point name.
AP Level VLAN ACL Mapping	
VLAN Id	VLAN ID.
Ingress ACL	Name of the Ingress ACL.
Egress ACL	Name of the Egress ACL.
Group Level VLAN ACL Mapping	
VLAN Id	VLAN ID.
Ingress ACL	Name of the Ingress ACL.
Egress ACL	Name of the Egress ACL.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

WebAuth and WebPolicy ACL Mappings for FlexConnect Access Points

Choose **WIRELESS > Access Points > All APs, >** *AP_name* **> FlexConnect** tab, and click the **External WebAuthentication ACLs** link to navigate to the External WebAuthentication ACLs page. This page enables you to configure WLAN ACL mappings for FlexConnect access points and to add WebPolicy ACLs.

This table describes the WebAuth and WebPolicy ACL mappings parameters.

Table 5-21   WebAuth and WebPolicy ACL Mappings for FlexConnect Access Points

Parameter	Description
AP Name	Name of the access point.
Base Radio MAC	MAC address of the 802.11a/b/g/n radio.
WLAN ACL Mapping	
WLAN ID	WLAN ID number.
WebAuth ACL	Drop-down list from which you can choose the FlexConnect ACL for external web authentication in locally switched WLANs. Click **Add** to configure the WLAN ACL Mapping.
WebPolicies	
WebPolicy ACL	Drop-down list from which you can select a FlexConnect ACL to be added as a web policy. Click **Add** to add the WebPolicy ACL. **Note** You can configure up to 16 WebPolicy ACLs that are specific to an access point.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Local Split ACL Mappings (for FlexConnect Access Points)

Choose **WIRELESS > Access Points > All APs, >** *AP_name* **> FlexConnect** tab, and click the **Local Split ACLs** link to navigate to the Local Split ACLs page. This page enables you to configure local split ACLs for FlexConnect access points.

This table describes the local split ACL mappings parameters.

Table 5-22   Local Split ACL Mappings for FlexConnect Access Points

Parameter	Description
AP Name	Name of the access point.
Base Radio MAC	MAC address of the 802.11a/b/g/n radio.
WLAN ACL Mapping	

Table 5-22   Local Split ACL Mappings for FlexConnect Access Points

Parameter	Description
WLAN ID	WLAN ID number.
Local-split ACL	Drop-down list from which you can choose the Local Split ACL to locally switch traffic in centrally switched WLANs. Click **Add** to configure the local split ACL mappings.
	Local-split configuration is applied specific to a WLAN. You can also apply this configuration from a FlexConnect group or from an AP. If the local-split configuration is applied at both the FlexConnect group level and AP level, then the configuration applied at the AP level has higher priority. In other words, the FlexConnect ACL specific to the AP has higher priority.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Central DHCP ACL Mappings for FlexConnect Access Points

Choose **WIRELESS > Access Points > All APs, >** *AP_name* **> FlexConnect** tab, and click the **Central DHCP Processing** link to navigate to the Central DHCP Processing page. This page enables you to configure central DHCP, override DNS, and enable NAT/PAT on a WLAN.

This table describes the central DHCP mappings parameters.

Table 5-23   Central DHCP Mappings for FlexConnect Access Points

Parameter	Description
AP Name	Name of the access point.
Base Radio MAC	MAC address of the 802.11a/b/g/n radio.
WLAN DHCP Mapping	
WLAN ID	WLAN ID number.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

VLAN Mappings for Mesh Access Points

Choose **WIRELESS > Access Points > All APs**, click the AP name of a mesh (bridge) access point, click the **Mesh** tab, and then click an Ethernet interface from the Ethernet Bridging area to navigate to the VLAN Mappings page.

Note   The Ethernet Bridging area appears after you enable Ethernet Bridging and click **Apply**.

Ethernet VLAN tagging allows specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN (access mode) or bridged to another wireless mesh network (trunk mode).

Configure access mode on gigabitEthernet1. Configure trunk mode on gigabitEthernet0.

Note   Configurations on gigabitEthernet2 and gigabitEthernet3 interfaces are not supported.

Configuring Access Mode

To configure a mesh access point (MAP) access port, follow these steps:

Step 1   Choose **access** from the mode drop-down list.

Step 2   Enter a VLAN ID. The VLAN ID can be any value between 1 and 4095.

Step 3   Click **Apply**.

Note   VLAN ID 1 is not reserved as the default VLAN.

Note   A maximum of 16 VLANs are supported across all of a RAP's subordinate MAPs.

Configuring Trunk Mode

To configure a root access point (RAP) or MAP trunk port, follow these steps:

Step 1   Choose **trunk** from the mode drop-down list.

Step 2   Enter a native VLAN ID for the incoming traffic. The native VLAN ID can be any value between 1 and 4095. Do not assign any value assigned to a user-VLAN (access).

Step 3   Click **Apply**.

A trunk VLAN ID text box and a summary of configured VLANs appears at the bottom of the page. The trunk VLAN ID text box is for outgoing packets.

Step 4   Enter a trunk VLAN ID for outgoing packets:

   a.   If forwarding untagged packets, do not change the default trunk VLAN ID value of zero (MAP-to-MAP bridging, campus environment).

   b.   If forwarding tagged packets, enter a VLAN ID (1 to 4095) that is not already assigned (RAP to switch on wired network).

Step 5   Click **Add** to add the trunk VLAN ID to the allowed VLAN list. The newly added VLAN appears under Configured VLANs on the page.

To remove a VLAN from the list, click the blue arrow adjacent the desired VLAN and choose **Remove**.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Neighbor Information of Access Points

Choose **WIRELESS > Access Points > All APs**, click the blue arrow adjacent the desired access point and choose **Neighbor Information** to navigate to the Neighbor Information page.

This page lists the parent, children, and neighbors of the access point. It provides each access point's name and radio MAC address.

To perform a link test between the access point and its parent or children, click the blue arrow adjacent the desired access point and choose **LinkTest**. A dialog box appears.

Click **Submit** to start the link test. The link test results appear on the Mesh > LinkTest Results page.

- To view the details for any access point on this page, click the blue arrow adjacent the desired access point your cursor over the blue drop-down arrow for the desired access point and choose **Details**. The Link Details of Access Points page appears.

- To view statistics for any access point on this page, click the blue arrow adjacent the desired access point and choose **Stats**. The Mesh Neighbor Statistics page appears.

Link Details of Access Points

Choose **WIRELESS > Access Points > All APs**, click the blue arrow adjacent the desired access point and choose **Details** to navigate to the Link Details page.

This page displays the following details:

- Neighbor Local Mode AP Fast Heartbeat Timeout (1 to 10)
- Neighbor MAC Address
- Neighbor Type
- Channel
- Backhaul Data Rate
- Link SNR
- Time of Last Hello

Mesh Neighbor Statistics

Choose **WIRELESS > Access Points > All APs**, click the blue arrow adjacent the desired access point and choose **Stats** to navigate to the Neighbor Statistics page.

This page displays the following details:

- Neighbor AP Name/MAC Address
- Neighbor Base Radio MAC Address
- Packets Transmitted as Parent
- Packets Received as Parent
- Total Tx Packets
- Total Tx Successful
- Total Tx Retries

- Poor SNR Rx

Access Points Statistics

Choose **WIRELESS > Access Points > All APs**, click the blue arrow adjacent the desired access point and choose **Statistics** to navigate to the Access Points Statistics page.

This page provides the following information:

- AP Role—Role of the access point in the mesh network RootAP or MeshAP
- Bridge Group Name—Name of the bridge group to which the access point belongs
- Backhaul Interface—Backhaul interface on which the access point operates
- Switch Physical Port—Number of the physical switch port

Mesh Node Stats

This table describes the mesh node parameters.

Table 5-24   *Mesh Node Parameters*

Parameter	Description
Malformed Neighbor Packets	Number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.
Poor Neighbor SNR Reporting	Number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.
Excluded Packets	Number of packets received from excluded neighbor mesh access points.
Insufficient Memory Reporting	Number of insufficient memory conditions.
Rx Neighbor Requests	Number of broadcast and unicast requests received from the neighbor mesh access points.
Rx Neighbor Responses	Number of responses received from the neighbor mesh access points.
Tx Neighbor Requests	Number of unicast and broadcast requests sent to the neighbor mesh access points.
Tx Neighbor Responses	Number of responses sent to the neighbor mesh access points.
Parent Changes Count	Number of times that a mesh access point (child) moves to another parent.
Neighbor Timeouts Count	Number of neighbor timeouts.

Queue Stats

This table describes the queue statistics.

Table 5-25   Queue Statistics Parameters

Parameter	Description
Gold Queue	Average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval.
Silver Queue	Average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval.
Platinum Queue	Average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval.
Bronze Queue	Average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval.
Management Queue	Average and peak number of packets waiting in the management queue during the defined statistics time interval.

Mesh Node Security Stats

This table describes the mesh node security statistics.

Table 5-26   Mesh Node Security Statistics Parameters

Parameter	Description
Transmitted Packets	Number of packets transmitted during security negotiations by the selected mesh access point.
Received Packets	Number of packets received during security negotiations by the selected mesh access point.
Association Request Failures	Number of association request failures that occur between the selected mesh access point and its parent.
Association Request Timeouts	Number of association request timeouts that occur between the selected mesh access point and its parent.
Association Requests Successful	Number of successful association requests that occur between the selected mesh access point and its parent.
Authentication Request Failures	Number of failed authentication requests that occur between the selected mesh access point and its parent.
Authentication Request Timeouts	Number of authentication request timeouts that occur between the selected mesh access point and its parent.
Authentication Requests Successful	Number of successful authentication requests between the selected mesh access point and its parent.
Reassociation Request Failures	Number of failed reassociation requests between the selected mesh access point and its parent.
Reassociation Request Timeouts	Number of reassociation request timeouts between the selected mesh access point and its parent.
Reassociation Requests Successful	Number of successful reassociation requests between the selected mesh access point and its parent.
Reauthentication Request Failures	Number of failed reauthentication requests between the selected mesh access point and its parent.

Table 5-26   Mesh Node Security Statistics Parameters

Parameter	Description
Reauthentication Request Timeouts	Number of reauthentication request timeouts that occur between the selected mesh access point and its parent.
Reauthentication Requests Successful	Number of successful reauthentication requests that occur between the selected mesh access point and its parent.
Unknown Association Requests	Number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.
Invalid Association Requests	Number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state may occur when the selected child is a valid neighbor but is not in a state that allows association.
Reauthentication Requests	Number of unknown reauthentication requests received by the parent mesh access point node from its child. This state may occur when a child mesh access point is an unknown neighbor.
Invalid Reauthentication Requests	Number of invalid reauthentication requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reauthentication.
Unknown Reassociation Requests	Number of unknown reassociation requests received by the parent mesh access point from a child. This state may occur when a child mesh access point is an unknown neighbor.
Invalid Reassociation Requests	Number of invalid reassociation requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reassociation.

Link Test

Choose **WIRELESS > Access Points > All APs/Detail,** and then click **Link Test** to navigate to the Link Test page.

You can test the status of a bridge connection using the link test. Using the link test, you can configure and execute tests, check the status of a test, and access test data.

This test involves one transmitting WRAP and one receiving WRAP. A WRAP can run only one test at a time; you cannot have multiple WRAPs transmitting to one receiving WRAP.

The link test page displays the link test parameters and the results of the last link tests, sorted by the link test ID. The link test ID is the receiving access point's ID.

This table describes the link test parameters.

Table 5-27   Link Test Parameters

Parameter	Description
AP Name	(Display Only Field) The transmitting WRAP name.
AP MAC address	(Display Only Field) The transmitting WRAP MAC address.
AP Role	(Display Only Field) The transmitting WRAP role.
Bridged Neighbor AP	WRAP whose link you want to test. This is the Link Test ID. Make sure to clear the existing link test results using the Clear option at the bottom of that WRAP's Link Test Results area. For example, if you are conducting the link test on Bridged Neighbor AP 8, go to the Link Test Results section, scroll to the Link Test ID 8, and click **Clear**.
Packet Size	Packet size. The range is from 0 to 2300.
Bytes per Second	Bytes per second. This value can be up to 80% of the data rate.
Duration in Seconds	Test duration. The range is from 10 to 300 seconds.
Data Rate (Mbps)	The valid data rates are as follows: • 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 • 802.11b: 1, 2, 5.5, 11 • 802.11g: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54

Note   Before conducting a link test on a receiving WRAP, go to the Link Test Results of that WRAP and click **Clear** to clear the existing Link Test Results.

Specify your link test values and click **Link Test**.

The link test is conducted for the duration that you specify. If the test is successful, the Link Test Results field parameters are populated with the latest link test results for the selected Bridged Neighbor AP (Link Test ID).

Link Test Results

This table lists the link test result parameters.

Table 5-28   Link Test Result Parameters

Parameter	Description
Link Test ID	Receiving WRAP ID specified using the Bridged Neighbor AP field.
Bridged Neighbor AP	Receiving WRAP whose link was tested.
Tx Packets	Number of packets transmitted during the link test duration.
Tx Dropped Packets	Number of transmitting packets dropped during the link test duration.
	The transmitting WRAP can only send data at a certain rate. If more data is received than can be sent, it is stored in the buffer. If the buffer is full, some packets are dropped.
Rx Good Packets	Number of good packets received during the link test duration.
Rx Lost Packets	Number of lost packets during the link test duration.
Rx Out of Order Packets	Number of packets received that were not in the order at which they were transmitted during the link test duration.
	Packets are received by the receiving WRAP in the order that they were sent by the transmitting WRAP. For example, the second packet transmitted is expected to reach the receiving WRAP as the second packet. If the packet that was sent second reaches the receiving WRAP after it received the forth packet, the second packet is an out of order packet.

802.11a/n/ac Radios

Choose **WIRELESS > Access Points > Radios > 802.11a/n/ac** or **MONITOR > Summary** and click **802.11 a/n/ac** radios to navigate to the 802.11 a/n/ac Radios page.

This page displays an overview of your 802.11a/n/ac Cisco Radio network. The status of each 802.11a/n/ac Cisco Radio configured on this Cisco WLC and its profile is detailed here.

Beginning in controller Release 7.5 and later, 802.11ac APs are supported in the controller. 802.11ac, a 5 GHz-only technology, is a faster and a more scalable version of 802.11n. The 802.11n inherits the properties of the 802.11n radio.

- To configure the identified Cisco Radio, click the blue arrow adjacent the desired radio and choose **Configure** (Configuring 802.11a/n APs).

- To view details about the identified Cisco Radio, click the blue arrow adjacent the desired radio and choose **Details** (802.11a/n/ac AP Interfaces Details).

Search AP Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) to create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access points by MAC addresses or AP names.

The current filter parameters are displayed in the Current Filter field.

- MAC Address—MAC address text box where you enter a MAC address.
- AP Name—AP Name text box where you enter an access point name.
- CleanAir Oper Status—Operational status of the CleanAir capable access point.

> **Note**   When you enable filtering by the MAC address, the other filters are disabled automatically. However, you can use a combination of the AP name and CleanAir operational status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the 802.11a/n/ac Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

> **Note**   If you want to remove the filter and display the entire access point list, click **Clear Filter**.

This table lists the 802.11 a/n/ac radio parameters.

Table 5-29   802.11 a/n/ac Cisco Radio Summary Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Radio Slot#	Slot in which the radio is installed. **Note** Radio slot 2 information for all the AP 3600 radios appears when the 802.11ac radio is plugged in.
Base Radio MAC	MAC address of the 802.11a/n/ac radio.
Sub Band	Radio sub band, if it is active. The value is 4.9 GHz or 5.8 GHz.
Admin Status	Admin status of the access point on this radio.
Operational Status	Cisco Radio operational status.
Channel	Channel number of the access point.
CleanAir Admin Status	Administration status of the spectrum sensor for the access point.

Table 5-29   802.11 a/n/ac Cisco Radio Summary Parameters

Parameter	Description
CleanAir Oper Status	Status of the spectrum sensor for this access point. The CleanAir status is one of the following: • UP—The spectrum sensor for the access point radio is operational (error code 0). • DOWN—The spectrum sensor for the access point radio is not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio. • ERROR—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable CleanAir functionality on the radio. • N/A—This access point radio cannot support CleanAir functionality. Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir. Note You can create a filter to make the 802.11a/n Radios page or the 802.11b/g/n Radios page show only access point radios that have a specific CleanAir status (such as UP, DOWN, ERROR, or N/A). This feature is especially useful if your list of access point radios spans multiple pages, preventing you from viewing them all at once. To create a filter, click **Change Filter** to open the Search AP page, select one or more of the CleanAir Status check boxes, and click **Find**. Only the access point radios that match your search criteria appear on the 802.11a/n Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, CleanAir Status: UP).
Radio Role	Radio role for the backhaul, either UPLINK or DOWNLINK.
Power Level	Transmit power level for the access point: • 1 = Maximum power allowed per Country Code setting • 2 = 50% power • 3 = 25% power • 4 = 6.25 to 12.5% power • 5 = 0.195 to 6.25% power Note The power levels and available channels are defined by the Country Code setting and are regulated on a country by country basis.
Antenna	Internal or external antennas.

Configuring 802.11a/n APs

Choose **WIRELESS > Access Points > Radios > 802.11a/n/ac**, click the blue arrow adjacent the desired access point and choose **Configure** to navigate to the Configure page. For details on configuring an 802.11ac radio on access points, see Configuring 802.11ac Radio in Access Points.

This page enables you to configure parameters specifically for this Cisco Radio including the antenna type, RF channel, and Tx power level assignments. The performance profile for this Cisco Radio is also accessed through this page.

General

This table describes the general 802.11a/n/ac parameters.

Table 5-30   General Parameters

Parameter	Description
AP Name	(Display Only Field) Customer-definable name of the access point.
Admin Status	Interface status of enabled or disabled. The default is enabled. **Note** If you disable 802.11n, the 802.11ac radio is also disabled.
Operational Status	(Display Only Field) Cisco Radio operational status: either UP or DOWN. The default is UP.
Slot #	Slot where the radio is installed.

Link Parameters

These parameters are displayed for the 802.11a/n/ac radios on the Mesh access points.

This table describes the link parameters.

Table 5-31   Link Parameters

Parameter	Description
Radio Role	Radio role for the backhaul of UPLINK or DOWNLINK.
Source Backhaul MAC	MAC address of the source backhaul radio.

11n Parameters

This table describes the 802.11n parameters.

Table 5-32   11n Parameters

Parameter	Description
11n Supported	(Display Only Field) Indicates whether 802.11n is supported.
11ac Supported	(Display Only Field) Indicates whether 802.11ac is supported. This field appears only for 802.11ac slave radios on slot 2.

Clean Air

This table describes the CleanAir configuration parameters.

Table 5-33   CleanAir Parameters

Parameter	Description
CleanAir Capable	(Display Only Field) CleanAir capability of the access point. Whether the access point is CleanAir capable.
CleanAir Admin Status	Status of the CleanAir admin that you can enable or disable. The default is disabled.

Antenna Parameters

This table describes the antenna parameters.

Table 5-34   Antenna Parameters

Parameter	Description
Antenna Type	Internal or external antenna type.
Antenna (Displayed if 11n is supported)	Specific antennae for the access point that you can enable or disable: • A—Right antenna port • B—Left antenna port • C—Center antenna port • D—Dua-band antenna By default, all are selected. For example, to enable transmissions from antenna ports A and B and receptions from antenna port C, you should select the following check boxes: Tx: A and B and Rx: C. Valid combinations are A, A+B, A+B+C, or A+B+C+D. When you select a dual-mode antenna, you can apply only a single spatial 802.11n stream rate. The range is from MCS 0 to 7. When you select two dual-mode antennae, you can apply only two spatial 802.11n stream rates: The range is from MCS 0 to 15. You must enable two antennae for dual-band access points such as Cisco Aironet 1600 Series Access Point and Cisco Aironet 3600 Series Access Point.

Table 5-34   Antenna Parameters

Parameter	Description
Diversity (Displayed if 11n is not supported)	Select one of the following: • Enable—Enables diversity on both the connectors. • Right—Enables diversity for the Right (Connector B) antenna. • Left—Enables diversity for the Left (Connector A) antenna.
Antenna Gain	Antenna gain. If you have a high-gain antenna, enter a value that is twice the actual dBi value (see the Cisco Aironet Antenna Reference Guide for antenna dBi values). Otherwise, enter 0. For example, if your antenna has a 4.4 dBi gain, multiply the 4.4 dBi by 2 and round down to enter only the whole number (8). The controller reduces the actual equivalent isotropic radiated power (EIRP) to make sure that the antenna does not violate your country's regulations. **Note** This option is available only if the antenna type is set to **external**.

Sniffer Channel Assignment

Note   This area is displayed if you set the AP Mode on the General Tab to Sniffer.

This table describes the sniffer channel assignment parameters.

Table 5-35   Sniffer Channel Assignment Parameters

Parameter	Description
Sniff	Sniffer operation that you can enable or disable. When enabled, the access point begins capturing and forwarding all the packets from the client on a specific channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). The default value is disabled (or unselected).
Channel	Channel on which the access points sniffs for packets. The default value is 1.
Server IP Address	IP address of the remote machine running Airopeek or Wireshark.

RF Channel Assignment

Note   This area is displayed if you set the AP Mode on the General Tab to Sniffer.

This table describes the RF channel assignment parameters.

Table 5-36   RF Channel Assignment Parameters

Parameter	Description
Current Channel	(Display Only Field) Channel number of the access point.
	Note The channels 1, 6, and 11 are nonoverlapping.
Channel Width[1]	Set the RF channel Assignment Method to Custom, and select one of the following channel widths:
	• 20 MHz—Enables the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels. This is the default value.
	• 40 MHz—Enables 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together. The radio uses the primary channel that you choose from the Assignment Method drop-down list as well as its extension channel for faster throughput. Each channel has only one extension channel (36 and 40 are a pair, 44 and 48 are a pair, and so on). For example, if you choose a primary channel of 44, the controller would use channel 48 as the extension channel. If you choose a primary channel of 48, the controller would use channel 44 as the extension channel.
	• 80 MHz—Enables the radio to communicate using 80-MHz channels. This option is supported only for 802.11ac capable radios. 802.11ac channelization uses four adjacent 20-MHz channels. From the drop-down list you can select the primary channel and based on the available channel pairing, appropriate secondary 20-MHz and secondary 40-MHz extension channels can be configured for the radio.
	Note To select the channel width as 80-MHz, 802.11ac support must be enabled in **WIRELESS > 802.11a/n/ac > High Throughput (802.11n/ac)**.
Assignment Method	Assignment method that you can choose:
	• Global—Use this setting if you set the channel of the access point globally by the Cisco WLC.
	• Custom—Use this setting if you set the channel locally. Choose a channel from the drop-down list.
	Note The assignment method should be left at the global setting to enable the Cisco WLC to dynamically change the channel number based Radio Resource Management (RRM) directives.
	For the Cisco 3600 Access Points with the 802.11ac module, channel and transmit power assignments are not supported in the custom mode. The 802.11ac radio inherits the channel and power assignments applied to the 802.11n radio. When the assignment mode is custom, you can configure only the channel width settings on the 802.11ac radio.

1. Statically configuring an access point's radio for the 20-MHz, 40-MHz, or 80-MHz mode overrides the globally configured DCA channel width setting on the 802.11a/n/ac Dynamic Channel Assignment page. If you ever change the static RF channel assignment method back to Global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

Tx Power Level Assignment

This table describes the Tx power level assignment parameters.

Table 5-37   Tx Power Level Assignment Parameters

Parameter	Description
Current Tx Power Level	(Display Only Field) Transmission power level of the access point. Tx Power Level indicates the maximum power. **Note** The power levels and available channels are defined by the Country Code setting and are regulated on a country-by-country basis.
Assignment Method	Assignment method that you can choose: • Global—Use this setting if you set the transmit power of the access point globally by the Cisco WLC. • Custom—Use this setting if the transmit power of the access point is set locally. Choose an option from the drop-down list.

Note   The assignment method should be left at the global setting to enable the Cisco WLC to dynamically change the transmit power level based on the Radio Resource Management (RRM).

Configuring Tx Power Levels

The Current Tx Power Level setting controls the maximum conducted transmit power. The maximum available transmit power varies according to the configured channel, individual country regulation, and access point capability. See the product guide or data sheet at http://www.cisco.com for each specific model in order to determine the access point capability.

The Current Tx Power Level setting of 1 represents the maximum conducted power setting for the access point. Each subsequent power level (for example, 2, 3, 4, and so on) represents approximately a 50 percent (or 3 dBm) reduction in the transmit power from the previous power level.

Note   The actual power reduction may vary slightly for different models of access points.

Based on the configured antenna gain, the configured channel, and the configured power level, the actual transmit power at the access point can be reduced so that the specific country regulations are not exceeded.

Note   Whether you choose the Global or Custom assignment method, the actual conducted transmit power at the access point is verified so that country specific regulations are not exceeded.

Performance Profile

See the Performance Profile of 802.11a/n/ac Access Points topic.

Tracking Optimization

Note If your access point is configured to operate in Monitor mode, you can enable tracking optimization on up to four channels within the 2.4 GHz band (802.11b/g radio) of an access point to enable you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6 and 11).

This table describes the tracking optimization parameters.

Table 5-38   Tracking Optimization Parameters

Parameter	Description
Enable Tracking Optimization	Tracking optimization that you can enable or disable.
Channel 1 Channel 2 Channel 3 Channel 4	Channels on which you want to monitor tags. **Note** To eliminate a channel from monitoring tag, choose **None** from the channel drop-down list.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Configuring 802.11ac Radio in Access Points

Beginning in Cisco WLC Release 7.5 and later, 802.11ac APs are supported by the Cisco WLC. 802.11ac, a 5 GHz-only technology, is a faster and a more scalable version of 802.11n.

Choose **WIRELESS > Access Points > Radios > 802.11a/n/ac**, click the blue arrow adjacent the desired 802.11ac slave radio on slot 2, and then click **Configure** to configure the 802.11ac slave radio.

802.11ac radio on slot 2 is a slave radio and you can configure only a few parameters specifically for this Cisco Radio. As 802.11ac is a slave radio, it inherits many properties from the main radio 802.11a/n on slot 1. The only parameters that you can configure for this radio are as follows:

- Admin Status—Interface status of the radio that can be enabled or disabled. The default is enabled. 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, or 80 MHz. If you choose the channel width as 80 MHz, you must enable 802.11ac mode in the High Throughput page. To enable 802.11ac mode, choose **WIRELESS > 802.11a/n/ac > High Throughput (802.11n/ac)**, and select the **11ac Mode** check box.

The 11ac Supported field is a nonconfigurable parameter that appears for the 802.11ac slave radio on slot 2 and indicates that the radio is 802.11ac capable.

For the Cisco 3600 Access Points with the 802.11ac module, channel and transmit power assignments are not supported in the custom mode. The 802.11ac radio inherits the channel and power assignments applied to the 802.11n radio. When the assignment mode is custom, you can configure only the channel width settings on the 802.11ac radio.

Performance Profile of 802.11a/n/ac Access Points

Choose **WIRELESS > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n**, click the blue drop-down arrow for an AP name, choose **Configure**, and then click **Performance Profile** to navigate to the Performance Profile page.

This page shows the details of the performance profile of the selected Cisco Radio.

This table describes the 802.11 parameters.

Table 5-39 **802.11 General Parameters**

Parameter	Description
Interface Type	Cisco Radio type: 802.11a/n/ac or 802.11b/g/n.
AP Name	User-definable name of the access point.
AP ID	Access point identification number that is automatically assigned by the Cisco WLC.
Profile Parameters Globally Controlled	Globally controlled parameters that you can enable or disable. You cannot change the following parameters if the Profile Parameters Globally Controlled check box is selected.
Interference (0 to 100%)	Foreign 802.11a/n or 802.11b/g/n interference threshold between 0 and 100 percent. You can globally set this setting on the 802.11a/n/ac RF Grouping and 802.11b/g/n RF Grouping pages.
Clients (1 to 75)	Client threshold between 1 and 75 clients. You can globally set this setting on the 802.11a/n/ac RF Grouping and 802.11b/g/n RF Grouping pages.
Noise (-127 to 0 dBm)	Noise threshold between −127 and 0 dBm. You can globally set this setting on the 802.11a/n/ac RF Grouping and 802.11b/g/n RF Grouping pages.
Coverage (3 to 50 dBm)	802.11a/n or 802.11b/g/n coverage threshold between 3 and 50 dBm. You can globally set this setting on the 802.11a/n/ac RF Grouping and 802.11b/g/n RF Grouping pages.
Utilization (0 to 100%)	802.11a/n or 802.11b/g/n RF utilization threshold between 0 and 100 percent. You can globally set this setting on the 802.11a/n/ac RF Grouping and 802.11b/g/n RF Grouping pages.
Coverage Exception Level (0 to 100%)	Coverage exception level between 0 and 100 percent. You can globally set this setting on the 802.11a/n/ac RF Grouping and 802.11b/g/n RF Grouping pages.
Data Rate (1 to 1000 Kbps)	802.11a/n or 802.11b/g/n throughput threshold between 1 Kbps and 1000 Kbps. You can globally set this setting on the 802.11a/n/ac RF Grouping and 802.11b/g/n RF Grouping pages.
Client Min Exception Level (1 to 75)	Client minimum exception level. You can globally set this setting on the 802.11a/n/ac RF Grouping and 802.11b/g/n RF Grouping pages.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11a/n/ac AP Interfaces Details

Choose **WIRELESS > Access Points > Radios > 802.11a/n/ac**, click the blue arrow adjacent the desired access point and choose **Detail** to navigate to the Details page.

This page primarily lists the read-only attributes of the selected Cisco Radio.

AP Details

✎
Note   The Monitor Mode parameter is not displayed for ODM access points.

This table describes the AP details.

Table 5-40   AP Details Parameters

Parameters	Description
Interface Type	Cisco Radio type 802.11a/n/ac.
AP Name	Name assigned to the access point.
AP ID	Identification number assigned when the access point is configured.
Admin Status	Interface status either enabled or disabled.
Operational Status	Cisco Radio operational status. The value is UP or DOWN.
11n Supported	Support of 11n. The value is Yes or No.
11ac Supported	Support of 802.11ac. The value is Yes or No.
Monitor Mode	Access point monitor mode: Local (normal operation), Cisco 1030 remote edge lightweight access point (Cisco 1030 IEEE 802.11a/b/g remote edge lightweight access point), or Monitor (monitor-only mode).
Location	User-definable location.

Station Configuration Parameters

The following parameters are not displayed for Cisco OEAP 600 Series access points:

- CFP Period
- CFP Max Duration

This table describes the station configuration parameters.

Table 5-41   Station Configuration Parameters

Parameters	Description
Configuration Type	Configuration type of Automatic or Custom.
Number of WLANs	Number of WLANs. 1 (one) is the default.
Medium Occupancy Limit	Maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.

Table 5-41   Station Configuration Parameters

Parameters	Description
CFP Period	DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	Maximum duration of the CFP in TU that may be generated by the PCF. It is modified by MLME-START.request primitive.
BSSID	MAC address of the access point.
Beacon Period	Rate at which the SSID is broadcast by the access point, from 100 to 600 milliseconds.
Country String	Country in which the station is operating. The first two octets of this string are the two-character country code.

Operation Rate Set

This table describes the operation rate parameters.

Table 5-42   Operation Rate Set Parameters

Parameter	Range
6000 Kilo Bits	Mandatory, Supported, or Disabled.
9000 Kilo Bits	Mandatory, Supported, or Disabled.
12000 Kilo Bits	Mandatory, Supported, or Disabled.
18000 Kilo Bits	Mandatory, Supported, or Disabled.
24000 Kilo Bits	Mandatory, Supported, or Disabled.
36000 Kilo Bits	Mandatory, Supported, or Disabled.
48000 Kilo Bits	Mandatory, Supported, or Disabled.
54000 Kilo Bits	Mandatory, Supported, or Disabled.

Note   The data rates set here are negotiated between the client and the Cisco WLC. If the data rate is set to Mandatory, the client must support it in order to use the network.

If a data rate is set as supported by the Cisco WLC, any associated client that also supports that same rate may communicate with the access point using that rate. It is not required that a client be able to use all the rates marked Supported in order to associate. Each data rate can also be set to Disabled to match client settings.

MAC Operation Parameters

This table describes the MAC operation parameters.

Table 5-43   MAC Operation Parameters

Parameter	Description
Configuration Type	Configuration type. Valid values are automatic or custom.
RTS Threshold	Attribute that indicates the number of octets in an MPDU, below which an RTS/CTS handshake is be performed. An RTS/CTS handshake shall be performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size turns off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value is 2347.
Short Retry Limit	Maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that is be made before a failure condition is indicated. The default value is 7.
Long Retry Limit	Maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value is 4.
Fragmentation Threshold	Current maximum size, in octets, of the MPDU that may be delivered to the PHY. An MSDU is broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU is fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute is the lesser of 2346 or the aMPDUMaxLength of the attached PHY and shall never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute is never less than 256.
Max. Tx MSDU Lifetime	Elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU is terminated. The default value is 512.
Max. Rx Life Time	Elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU. Further attempts to reassemble the MMPDU or MSDU are terminated. The default value is 512.

Tx Power

The following parameters are not displayed for Cisco OEAP 600 Series access points:

- Supported Power Levels
- Tx Power Configuration
- Current Tx Power Configuration Level

This table describes the Tx power parameters.

Table 5-44   Tx Power Parameters

Parameter	Description
# Supported Power Levels	Eight or fewer power levels, depending on operator preference.
Tx Power Level 1	Maximum power level that exists across all of the data rates (AP1505 or AP1510 only).
Tx Power Level 2	Tx Power Level 1 minus 3 dBm (AP1505 or AP1510 only).
Tx Power Configuration	Globally controlled or customized for this access point.
Current Tx Power Level	Operating transmit power level from the transmit power table.

Physical Channel Parameters

The following parameters are not displayed for the ODM access point:

- Configuration
- Current CCA Mode
- ED/TI Threshold

This table describes the physical channel parameters.

Table 5-45   Physical Channel Parameters

Parameter	Description
Current Channel	Current operating frequency channel.
Configuration	Locally customized or globally controlled.
Current CCA Mode	CCA method in operation. Valid values are as follows: • Energy detect only (edonly) = 01 • Carrier sense only (csonly) = 02 • Carrier sense and energy detect (edandcs) = 04 • Carrier sense with timer (cswithtimer) = 08 • High rate carrier sense and energy detect (hrcsanded) = 16
ED/TI Threshold	Energy Detect and Threshold that is used to detect a busy medium (frequency). CCA reports a busy medium upon detecting the RSSI above this threshold.

RF Recommendation Parameters

This table describes the RF recommendation parameters.

Table 5-46   RF Recommendation Parameters

Parameter	Description
Channel	802.11a/n Low Band, Medium Band, and High Band.
	802.11b/g/n.
Tx Power Level	0 if Radio Resource Management (RRM) is disabled.
	1 - 5 if Radio Resource Management (RRM) is enabled.
RTS/CTS Threshold	0 if Radio Resource Management (RRM) is disabled,
	1 - 5 if Radio Resource Management (RRM) is enabled.
	Refer to RTS Threshold in MAC Operation Parameters above.
Fragmentation Threshold	0 if Radio Resource Management (RRM) is disabled, or as Radio Resource Management (RRM) recommends.
Antenna Pattern	0 if Radio Resource Management (RRM) is disabled, or as Radio Resource Management (RRM) recommends.
Enhanced Local Mode (ELM) Parameters	
Promiscuous Mode Dwelling	Percentage of time that the access point spent in promiscuous mode. From Release 7.4 and later releases, the ELM can be in promiscuous mode for data frames too.
	This field appears only if the access point is in ELM mode.

802.11b/g/n Radios

Choose **WIRELESS > Access Points > Radios > 802.11b/g/n** or **MONITOR > Summary** and click **Detail** in the **802.11b/g/n Radios** row under the Access Point Summary section to navigate to the 802.11b/g/n Radios page.

This page displays an overview of your 802.11b/802.11g Cisco Radio network. The status of each 802.11b/g Cisco Radio configured on this Cisco WLC and its profile is detailed in the following table.

- To configure the identified Cisco Radio, click the blue arrow adjacent the desired radio and choose **Configure** (Configuring 802.11b/g/n Radios).

- To view details about the identified Cisco Radio, click the blue arrow adjacent the desired radio and choose **Details** (802.11b/g/n AP Interfaces Details).

Search AP Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access points by MAC addresses or AP names. The current filter parameters are displayed in the Current Filter field.

- MAC Address—MAC address text box.

- AP Name—Access point name text box.

- CleanAir Oper Status—Operational status of the CleanAir capable access point**.**

> **Note** When you enable filtering by the MAC address, the other filters are disabled. However, you can use a combination of the AP Name and CleanAir Oper Status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

> **Note** If you want to remove the filter and display the entire access point list, click **Clear Filter**.

802.11b/g/n Radio Summary

This table describes the 802.11 b/g/n radio summary parameters.

Table 5-47   802.11 b/g/n Radio Summary Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Radio Slot#	Slot where the radio is installed.
Base Radio MAC	Media Access Control address of the 802.11b/g/n radio.
Admin Status	Interface status of the access point on this radio. The values are enabled or disabled.
Operational Status	Cisco Radio operational status. The values are UP or DOWN.
Channel	Channel number of the access point. **Note** The channels 1, 6, and 11 are nonoverlapping.
CleanAir Admin Status	Administration status of the spectrum sensor for the access point.

Table 5-47   802.11 b/g/n Radio Summary Parameters

Parameter	Description
CleanAir Oper Status	Status of the spectrum sensor for this access point. The CleanAir status is one of the following: • UP—The spectrum sensor for the access point radio is currently operational (error code 0). • DOWN—The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio. • ERROR—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable CleanAir functionality on the radio. • N/A—This access point radio cannot support CleanAir functionality. Currently, only Cisco Aironet 3500 series access point radios can be configured for Cisco CleanAir. **Note** You can create a filter to make the 802.11a/n Radios page or the 802.11b/g/n Radios page show only access point radios that have a specific CleanAir status (such as UP, DOWN, ERROR, or N/A). This feature is especially useful if your list of access point radios spans multiple pages, preventing you from viewing them all at once. To create a filter, click **Change Filter** to open the Search AP page, select one or more of the CleanAir Status check boxes, and click **Find**. Only the access point radios that match your search criteria appear on the 802.11a/n Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, CleanAir Status: UP).
Power Level	Transmit power level of the access point where • 1 = Maximum power allowed per Country Code setting • 2 = 50% power • 3 = 25% power • 4 = 6.25 to 12.5% power • 5 = 0.195 to 6.25% power. **Note** The power levels and available channels are defined by the Country Code setting and are regulated on a country by country basis.
Antenna	Internal or external antennas.

Configuring 802.11b/g/n Radios

Choose **WIRELESS > Access Points > Radios > 802.11b/g/n**, and then click the blue arrow adjacent the desired access point and choose **Configure** to navigate to the Configure page.

This page enables you to configure parameters specifically for this Cisco Radio including antenna type, RF channel, and Tx power level assignments. The performance profile for this Cisco Radio is also accessed through this page.

General

This table describes the 802.11b/g/n parameters.

Table 5-48   General Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Admin Status	Administration interface status. The default is enabled.
Operational Status	Cisco Radio operational status.
Slot #	Slot where this radio is installed.

11n Parameters

This table describes the 802.11n parameters.

Table 5-49   11n Parameters

Parameter	Description
11n Supported	Indicates whether 11n is supported or not.

Clean Air

Note   Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

This table describes the CleanAir parameters.

Table 5-50   CleanAir Parameters

Parameter	Description
CleanAir Capable	Indicates whether the access point is CleanAir capable.
CleanAir Admin Status	Administration status of the spectrum sensor for the access point that you can enable or disable. Set this field to Enable or Disable from the drop-down list.

Antenna Parameters

This table describes the antenna parameters.

Table 5-51   Antenna Parameters

Parameter	Description
Antenna Type	Internal or External.
Antenna (Displayed if 11n is supported)	Internal or external antennae: • A—Right antenna port • B—Left antenna port • C—Center antenna port For example, to enable transmissions from antennae ports A and B and receptions from antenna port C, you should select the following check boxes: Tx: A and B and Rx: C.
Diversity (Displayed if 11n is not supported)	Select one of the following: For internal antennas: • Enable—Enables diversity on both Side A and Side B. • Side A—Enables diversity for the front (door) antenna. • Side B—Enable diversity for the rear antenna. For external antennas: • Enable—Enables diversity on both the connectors. • Right—Enables diversity for the Right (Connector B) antenna. • Left—Enables diversity for the Left (Connector A) antenna.
Antenna Gain	Actual—Cannot be set.

Sniffer Channel Assignment

Note This area is displayed if you set the AP Mode on the General Tab to Sniffer.

This table describes the sniffer channel assignment parameters.

Table 5-52   Sniffer Channel Assignment Parameters

Parameter	Description
Sniff	Sniffer operation that you can enable or disable. When enabled, the access point begins capturing and forwarding all the packets from the client on a specific channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). The default value is disabled (or unselected).
Channel	Channel on which the access points sniffs for packets. The default value is 1.
Server IP Address	IP address of the remote machine running Airopeek or Wireshark.

RF Channel Assignment

This table describes the RF channel assignment parameters.

Table 5-53   RF Channel Assignment Parameters

Parameter	Description
Current Channel	Channel number of the access point.
	Note The channels 1, 6, and 11 are nonoverlapping.
Current Width	RF channel Assignment Method and TX power level Assignment Method that you set to Custom, and choose the channel width.
	• 20 MHz—Enables the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels. This is the default value.
Assignment Method	Assignment method that you can choose:
	• Global—Use this setting if your access point's channel is set globally by the Cisco WLC.
	• Custom—Use this setting if you set the channel locally.
Note The assignment method should normally be left at the global setting to enable the Cisco WLC to dynamically change the channel number based Radio Resource Management (RRM) directives.	

Tx Power Level Assignment

This table describes the Tx power level parameters.

Table 5-54   Tx Power Level Assignment Parameters

Parameter	Description
Current Tx Power Level	Transmit power level of the access point. Tx Power Level indicates the maximum power.
	Note The power levels and available channels are defined by the Country Code setting and are regulated on a country by country basis.
Assignment Method	Assignment method that you can choose:
	• Global—Use this setting if your access point's transmit power is set globally by the Cisco WLC.
	• Custom—Use this setting if your access point's transmit power is set locally. Choose an option from the drop-down list.
Note The assignment method should be left at the global setting to enable the Cisco WLC to dynamically change the transmit power level based on the Radio Resource Management (RRM).	

Configuring Tx Power Levels

The Current Tx Power Level setting controls the maximum conducted transmit power. The maximum available transmit power varies according to the configured channel, individual country regulation, and access point capability. See the product guide or data sheet at http://www.cisco.com for each specific model in order to determine the access point capability.

The Current Tx Power Level setting of 1 represents the maximum conducted power setting for the access point. Each subsequent power level (for example, 2, 3, 4, and so on) represents approximately a 50-percent (or 3 dBm) reduction in the transmit power from the previous power level.

Note   The actual power reduction may vary slightly for different models of access points.

Based on the configured antenna gain, the configured channel, and the configured power level, the actual transmit power at the access point can be reduced so that the specific country regulations are not exceeded.

Note   Whether you choose the **Global** or **Custom** assignment method, the actual conducted transmit power at the access point is verified so that country specific regulations are not exceeded.

Performance Profile

See the Performance Profile of 802.11a/n/ac Access Points page.

Tracking Optimization

Note   If your access point is configured to operate in Monitor mode, you can enable tracking optimization on up to four channels within the 2.4 GHz band (802.11b/g radio) of an access point to enable you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6 and 11).

This table describes the tracking optimization parameters.

Table 5-55   Tracking Optimization Parameters

Parameter	Description
Enable Tracking Optimization	Tracking optimization.
Channel 1 Channel 2 Channel 3 Channel 4	Channels on which you want to monitor tags. **Note** To eliminate a channel from monitoring tags, choose **None** from the channel drop-down list.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11b/g/n AP Interfaces Details

Choose **WIRELESS > Access Points > Radios > 802.11b/g/n** and then click **Detail** to navigate to the Details page.

This page lists primarily read-only attributes of the selected Cisco Radio.

AP Details

This table describes the AP details.

Table 5-56   AP Details Parameters

Parameters	Description
Interface Type	Cisco Radio type as 802.11b/g/n.
AP Name	Name assigned to the access point.
AP ID	Identification number assigned when the access point is configured.
Admin Status	Interface status that you can enable or disable.
Operational Status	Cisco Radio operational status.
11n Supported	Support of 11n.
Monitor Mode	Access point Monitor mode: Local (normal operation), Cisco 1030 remote edge lightweight access point (Cisco 1030 IEEE 802.11a/b/g remote edge lightweight access point), or Monitor (monitor-only mode).
Location	User-definable location.

Station Configuration Parameters

This table describes the station configuration parameters.

Table 5-57   Station Configuration Parameters

Parameters	Description
Configuration Type	Configuration type of automatic or custom.
Number of WLANs	Number of WLANs. 1 (one) is the default.
Medium Occupancy Limit	Maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	Number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	Maximum duration of the CFP in TU that may be generated by the PCF. It is modified by MLME-START.request primitive.
BSSID	MAC address of the access point.

Table 5-57   Station Configuration Parameters

Parameters	Description
Beacon Period	Rate at which the SSID is broadcast by the access point, from 100 to 600 milliseconds.
Country String	Country in which the station is operating. The first two octets of this string are the two-character country code.

Operation Rate Set

This table describes the operation rate set parameters.

Table 5-58   Operation Rate Set Parameters

Parameter	Band	Range
1000 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported, or Disabled.
2000 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported, or Disabled.
5500 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported, or Disabled.
11000 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported, or Disabled.
6000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
9000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
12000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
18000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
24000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
36000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
48000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
54000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.

The data rates set are negotiated between the client and the controller. If the data rate is set to Mandatory, the client must support it in order to use the network.

If a data rate is set as Supported by the controller, any associated client that also supports that same rate may communicate with the Cisco Aironet 1000 Series IEEE 802.11a/b/g lightweight access point using that rate. It is not required that a client be able to use all the rates marked Supported in order to associate. Each data rate can also be set to Disabled to match Client settings.

MAC Operation Parameters

This table describes the MAC operation parameters.

Table 5-59   MAC Operation Parameters

Parameter	Description
Configuration Type	Configuration type of automatic or custom.
RTS Threshold	Attribute that indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed. An RTS/CTS handshake is performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size turns off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default is 2347.
Short Retry Limit	Maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that is made before a failure condition is indicated. The default is 7.
Long Retry Limit	Maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that is made before a failure condition is indicated. The default is 4.
Fragmentation Threshold	Current maximum size, in octets, of the MPDU that may be delivered to the PHY. An MSDU is broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU is fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute is the lesser of 2346 or the aMPDUMaxLength of the attached PHY and will never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute is never be less than 256.
Max. Tx MSDU Lifetime	Elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU is terminated. The default value is 512.
Max Rx Life Time	Elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU. Further attempts to reassemble the MMPDU or MSDU are terminated. The default is 512.

This table describes the Tx power parameters.

Table 5-60   Tx Power Parameters

Parameter	Description
# Supported Power Levels	Eight or fewer power levels, depending on operator preference.
Tx Power Configuration	Globally controlled or Customized for this access point.
Current Tx Power Level	Operating transmit power level from the transmit power table.

Physical Channel Parameters

This table describes the physical channel parameters.

Table 5-61   Physical Channel Parameters

Parameter	Description
Current Channel	Current operating frequency channel.
Configuration	Locally customized or globally controlled.
Current CCA Mode	CCA method in operation. Valid values are as follows: • Energy detect only (edonly) = 01 • Carrier sense only (csonly) = 02 • Carrier sense and energy detect (edandcs) = 04 • Carrier sense with timer (cswithtimer) = 08 High rate carrier sense and energy detect (hrcsanded) =16.
ED/TI Threshold	Energy Detect and Threshold that is used to detect a busy medium (frequency). CCA reports a busy medium upon detecting the RSSI above this threshold.

RF Recommendation Parameters

This table describes the RF recommendation parameters.

Table 5-62   RF Recommendation Parameters

Parameter	Description
Channel	802.11a/n Low Band, Medium Band, and High Band. 802.11b/g/n
Tx Power Level	0 if Radio Resource Management (RRM) is disabled. 1- 5 if Radio Resource Management (RRM)is enabled.
RTS/CTS Threshold	0 if Radio Resource Management (RRM) is disabled. 1 - 5 if Radio Resource Management (RRM) is enabled. See Threshold in MAC Operation Parameters above.
Fragmentation Threshold	0 if Radio Resource Management (RRM) is disabled, or as Radio Resource Management (RRM) recommends.
Antenna Pattern	0 if Radio Resource Management (RRM) is disabled, or as Radio Resource Management (RRM) recommends.

Enhanced Local Mode (ELM) Parameters

This table describes the ELM parameters.

Table 5-63   ELM Parameters

Parameter	Description
Promiscuous Mode Dwelling	Percentage of time that the access point spent in promiscuous mode. Beginning in controller Release 7.4 and later, the ELM can be in promiscuous mode for data frames too.
	This field appears only if the access point is in the Local mode or the Flexconnect mode, and the submode is WIPS.

CleanAir Parameters

The CleanAir operational status is displayed by the **Operational Status** parameter.

Persistent Devices

Note   Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

This table describes the persistent device parameters.

Table 5-64   Persistent Device Parameters

Parameter	Description
Class Type	Class type of the persistent device.
Channel	Channel that the device is affecting.
DC (%)	Duty cycle (in percentage) of the persistent device.
RSSI(dBm)	Received Strength Signal Indicator of the persistent device.
Last Seen Time	Timestamp when the device was last active.

Dual-Band Radios

Choose **WIRELESS > Access Points > Radios > Dual-Band Radios** or **MONITOR > Summary** and click **Detail** in the **Dual-Band Radios** row under the Access Point Summary section to navigate to this page.

This page displays an overview of your 802.11a/b/g Cisco Radio network. The status of each 802.11a/b/g Cisco Radio configured on this Cisco WLC and its profile is detailed in the following table.

- To configure the identified Cisco Radio, click the blue arrow adjacent the desired access point and choose **Configure** (Configuring Dual-Band Radios).

- To view details about the identified Cisco Radio, click the blue arrow adjacent the desired access point and choose **Details** (Dual-Band Radios Details).

Search AP Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access points by MAC addresses or AP names. The current filter parameters are displayed in the Current Filter field.

- MAC Address—MAC address text box.
- AP Name—Access point name text box.
- CleanAir Oper Status—Operational status of the CleanAir capable access point**.**

> **Note**   When you enable filtering by the MAC address, the other filters are disabled. However, you can use a combination of the AP Name and CleanAir Oper Status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the Dual-Band Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

> **Note**   If you want to remove the filter and display the entire access point list, click **Clear Filter**.

Dual-Band Radios Summary

This table describes the dual-band radios parameters.

Table 5-65   Dual-Band Radios Summary Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Radio Slot#	Slot where the radio is installed.
Base Radio MAC	Media Access Control address of the 802.11b/g/n radio.
Admin Status	Interface status of the access point on this radio. The values are enabled or disabled.
Operational Status	Cisco Radio operational status. The values are UP or DOWN.
CleanAir Admin Status	Administration status of the spectrum sensor for the access point.

Table 5-65   Dual-Band Radios Summary Parameters

Parameter	Description
CleanAir Oper Status	Status of the spectrum sensor for this access point. The CleanAir status is one of the following: • UP—The spectrum sensor for the access point radio is currently operational (error code 0). • DOWN—The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio. • ERROR—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable CleanAir functionality on the radio. • N/A—This access point radio cannot support CleanAir functionality. Currently, only Cisco Aironet 3500 series access point radios can be configured for Cisco CleanAir. **Note** You can create a filter to make the Dual-Band Radios page show only access point radios that have a specific CleanAir status (such as UP, DOWN, ERROR, or N/A). This feature is especially useful if your list of access point radios spans multiple pages, preventing you from viewing them all at once. To create a filter, click **Change Filter** to open the Search AP page, select one or more of the CleanAir Status check boxes, and click **Find**. Only the access point radios that match your search criteria appear on the Dual-Band Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, CleanAir Status: UP).
Antenna	Internal or external antennas.

Configuring Dual-Band Radios

Choose **WIRELESS > Access Points > Radios > Dual-Band Radios**, and click the blue arrow adjacent the desired access point and choose **Configure** to navigate to the Configure page.

This page enables you to configure parameters specifically for this Cisco Radio including antenna type, RF channel, and Tx power level assignments. The performance profile for this Cisco Radio is also accessed through this page.

General

This table describes the dual-band radios general parameters.

Table 5-66   General Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Admin Status	Administration interface status. The default is enabled.

Table 5-66   General Parameters

Parameter	Description
Operational Status	Cisco Radio operational status.
Slot #	Slot where this radio is installed.

11n and 11ac Parameters

This table describes the 802.11n and 802.11ac parameters.

Table 5-67   11n and 11ac Parameters

Parameter	Description
11n Supported	Whether 11n is supported or not.
11ac Supported	Whether 11ac is supported or not.

Clean Air

Note   Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

This table describes the CleanAir parameters.

Table 5-68   CleanAir Parameters

Parameter	Description
CleanAir Capable	Whether the access point is CleanAir capable.
CleanAir Admin Status	CleanAir Administration status of the spectrum sensor for the access point that you can enable or disable. You can set this field to the following options: • Enable—Enables CleanAir for both 2.4-GHz and 5-GHz radios. • Disable—Disables CleanAir for both 2.4-GHz and 5-GHz radios. • 2.4-GHz—Enables CleanAir only for 2.4-GHz radio. • 5-GHz—Enables CleanAir only for 5-GHz radio.

Dual-Band Radios Details

Choose **WIRELESS > Access Points > Radios > Dual-Band Radios** and then click **Detail** to navigate to the Dual-Band Radios page.

This page lists primarily read-only attributes of the selected Cisco Radio.

AP Details

This table describes the AP parameters.

Table 5-69   AP Details Parameters

Parameters	Description
Interface Type	Cisco Radio type as 802.11a/b/g/n.
AP Name	Name assigned to the access point.
AP ID	Identification number assigned when the access point is configured.
Admin Status	Interface status that you can enable or disable.
Operational Status	Cisco Radio operational status.
11n Supported	Support of 11n.
Monitor Mode	Access point Monitor mode: Local (normal operation), Cisco 1030 remote edge lightweight access point (Cisco 1030 IEEE 802.11a/b/g remote edge lightweight access point), or Monitor (monitor-only mode).
Location	User-definable location.

CleanAir Parameters

The CleanAir operational status is displayed by the **Operational Status** parameter.

Global Configuration

Choose **WIRELESS > Access Points > Global Configuration** to navigate to the Global Configuration page. This page enables you to configure the following parameters:

General

LED State—Check box and drop-down list to enable or disable the LED state of the access points. When you have many APs deployed and want to locate a specific AP, you can disable the LED state of all APs and then enable the LED state of the AP you are looking for. Thus, the AP that has its LED state enabled is easily identifiable.

Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is used between the network devices to discover properties of the other end of an interface and the device. When CDP is enabled on an interface, the device sends its properties and interface information to the device at the other end of the interface. The controller has an option to enable or disable CDP on all or a specific access point. This configuration is applied to the global CDP state on the access point.

Note   CDP over radio interface is applicable only for mesh APs.

This table describes the CDP parameters.

Table 5-70   CDP Parameters

Parameter	Description
CDP State	Global CDP that you can enable or disable on Ethernet or radio interfaces for all the access points currently associated to the controller.
Ethernet Interface#	Ethernet interface number.
CDP State (ethernet interface)	CDP that you can enable or disable for all or specific Ethernet interfaces on all or specific access points. **Note** Global CDP for the particular access points should be enabled before enabling or disabling the CDP state.
Radio Slot#	Slot where the radio is installed.
CDP State (radio slot)	CDP that you can enable or disable for all or specific radio interfaces on all or specific access points.

Login Credentials

Cisco IOS access points are shipped from the factory with "Cisco" as the default enable password. This password allows users to log in to the unprivileged mode and execute **show** and **debug** commands, which poses a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the access point's console port.

Note   You must keep careful track of the credentials used by the access points. Otherwise, you might not be able to log in to an access point's console port. If you need to return the access points to the default *Cisco/Cisco* username and password, you must clear the controller's configuration and the access point's configuration to return them to the default settings. To clear the controller's configuration, choose **Commands** > **Reset to Factory Default** > **Reset** on the controller GUI, or enter the **clear config** command on the controller CLI. To clear the access point's configuration, enter the **clear ap config command** *Cisco_AP* on the controller CLI. After the access point rejoins a controller, it adopts the default *Cisco/Cisco* username and password.

You can set a global username, password, and enable password that all access points inherit as they join the controller including access points that are currently joined to the controller and any that join in the future. You can override the global credentials and assign a unique username, password, and enable password for a specific access point. The following are requirements enforced on the password:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain the management username or the reverse of the username.
- The password should not contain words like Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o, or substituting $ for s.

This table describes the login credentials parameters.

Table 5-71   Login Credentials Parameters

Parameter	Description
Username	Username that is to be inherited by all access points that join the controller.
Password	Password that is to be inherited by all access points that join the controller.
Enable Password	Enable password that is to be inherited by all access points that join the controller.

Note   You can override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point by selecting the **Over-ride Global credentials** check box on the Credentials tab on the All APs Details page.

802.1X Supplicant Credentials

You can configure 8021.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning.

You can set global authentication settings that all access points inherit as they join the controller, which includes all access points that are currently joined to the controller and any that join in the future. If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.

This table describes the 802.1X supplicant credentials parameters.

Table 5-72   802.1X Supplicant Credentials Parameters

Parameter	Description
802.1X Authentication	Username, Password, and Confirm Password fields.
Username	Username that is to be inherited by all access points that join the controller.
Password	Password that is to be inherited by all access points that join the controller.
Confirm Password	Confirmed password that is to be inherited by all access points that join the controller.

Note   You can override the global authentication settings for a specific access point and assign a unique username and password to this access point by selecting the **Over-ride Global credentials** check box on the Credentials tab on the All APs Details page.

AP Failover Priority

You can configure high-priority access points so that the backup controller recognizes and accepts those access points first, even if it means disassociating a lower-ranked device as a means to provide an available port.

- Global AP Failover Priority—Access point priority assignments.

You can assign priorities to the access points on the High Availability tab on the All APs Details page. By default, all access points are set to priority level 1, which is the lowest priority level. Therefore, you need to assign a priority level only to those access points that warrant a higher priority.

AP Image Predownload

You can predownload images for all access points that are associated to your controller on the network.

This table describes the AP image predownload parameters.

Table 5-73   AP Image Predownload Parameters

Parameter	Description
Download Primary	Instruct all access points to download a primary image from the controller.
Download Backup	Instruct all access points to download an image from the controller and store it as a backup.
Interchange Image	Instruct all access points to swap their primary and backup images.

High Availability

You can configure primary and secondary backup controllers for all access points (which are used if primary, secondary, or tertiary controllers are not responsive) in this order: primary, secondary, tertiary, primary backup, and secondary backup. In addition, you can configure various timers, including heartbeat timers and discovery request timers. To reduce the controller failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller.

Note   You can configure the fast heartbeat timer only for access points in local and FlexConnect modes.

- AP Heartbeat Timeout—AP Heartbeat timeout value that you can enter. The valid range is 10 to 30 for the Cisco 7500 Series Controller and 1 to 30 for other platforms.

- Local Mode AP Fast Heartbeat Timer State—Fast heartbeat timer that you can enable or disable for access points in local mode. The default is disable.

- Local Mode AP Fast Heartbeat Timeout—If you enabled Local Mode AP Fast Heartbeat Timer, enter the timeout interval for this parameter. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure. The range for the AP Fast Heartbeat Timeout

value for Cisco Flex 7500 Controllers is 10–15 (inclusive) and is 1–10 (inclusive) for other controllers. The default value for the heartbeat timeout for Cisco Flex 7500 Controllers is 10. The default value for other controllers is 1 second.

- FlexConnect Mode AP Fast Heartbeat Timer State—Fast heartbeat timer for FlexConnect access points that you can enable or disable. The default is disable.

- FlexConnect Mode AP Fast Heartbeat Timeout—If you enabled the FlexConnect mode AP fast heartbeat timer, enter the interval (in seconds) for the fast heartbeat timer for FlexConnect access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure. The range for the FlexConnect Mode AP Fast Heartbeat Timeout value for Cisco Flex 7500 Controllers is 10–15 (inclusive) and is 1–10 for other controllers. The default value for the heartbeat timeout for Cisco Flex 7500 Controllers is 10. The default value for other controllers is 1 second.

- AP Primary Discovery Timeout—Timeout that you can set. Enter a number between 30 and 3600 seconds (inclusive) to configure the access point primary discovery request timer. The default value is 120 seconds.

- Back-up Primary Controller IP Address—IPv4/IPv6 address of the primary backup controller. From Release 8.0, controller supports IPv6.

Note   The default for the IP address is 0.0.0.0, which disables the primary backup controller.

- Back-up Primary Controller Name—Name of the primary backup controller.

- Back-up Secondary Controller IP Address—IP4/IPv6 address of the secondary backup controller. From Release 8.0, controller supports IPv6.

Note   The default value for the IP address is 0.0.0.0, which disables the secondary backup controller.

- Back-up Secondary Controller Name—Name of the secondary backup controller.

TCP MSS

If the client's maximum segment size (MSS) in a Transmission Control Protocol (TCP) three-way handshake is greater than the maximum transmission unit can handle, the client might experience reduced throughput and the fragmentation of packets. To avoid this problem in controller software release 6.0 or later releases, you can specify the MSS for all access points that are joined to the controller or for a specific access point.

When you enable this feature, the access point selects the MSS for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

- Global TCP Adjust MSS—Enable the check box and set the MSS for all access points that are associated with the controller.

    From Release 8.0, the controller supports IPv6. Use the following Global TCP Adjust MSS values for:

    - IPv4—Specify a value between 536 and 1363.

    - IPv6—Specify a value between 1220 and 1331.

> **Note** Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP.

AP Retransmit Config Parameters

When a controller goes out of service, the access point associated with it falls back to the next available controller. Before associating itself to a new controller, the access point first tries to establish a connection with the existing controller that it is associated with. It does so by sending a request (known as a retransmission) at regular intervals to the controller and for a specified number of times (retry count). If the access point does not get an acknowledgement from the controller, it tries to associate itself to the next available controller.

> **Note** Retransmission intervals and retry counts are not applicable for mesh access points.

You can configure the retransmission intervals and retry counts both at a global as well as a specific access point level. A global configuration applies these configuration parameters to all the access points. That is, the retransmission interval and the retry count would be uniform for all access points. Alternatively, when you configure the retransmission level and retry counts at a specific access point level, the values are applied to that particular access point. Access point specific configurations have higher precedence compared to Cisco WLC global configurations.

This table describes the AP retransmit config parameters.

Table 5-74   AP Retransmit Config Parameters

Parameter	Description
AP Retransmit Count	Number of times that you want the access point to retransmit the request to controller and vice-versa. Valid range is between 3 and 8.
AP Retransmit Interval	Time duration between retransmission of requests. Valid range is between 2 and 5.

OEAP Config Parameters

This table describes the Cisco 600 Series OfficeExtend Access Point (OEAP) config parameters.

Table 5-75   OEAP Config Parameters

Parameter	Description
Disable Local Access	Check box that you can select to disable access to the local GUI, LAN ports, and local SSID of the Cisco 600 Series OEAP.
Disable Split Tunnel	Check box that you can select to disable split tunnelling for Cisco 600 Series OEAP. Selecting the checkbox disables splitting the tunnel for all WLANs and remote LANs.

Flexconnect Ethernet Fallback

This table describes the FlexConnect Ethernet Fallback parameter.

Table 5-76   FlexConnect Ethernet Fallback Parameters

Parameter	Description
Radio Interface Shutdown	Check box that you can select to enable an AP radio interface or disable an AP radio interface. This is disabled by default.
	When the user selects this checkbox and when AP Ethernet Link goes down, the AP radio interface shuts down.
Delay (0 to 10 Sec)	Delay value, in seconds. The value range is between 0 and 10. The default is 0.

Global Telnet SSH

This table describes the Global Telnet SSH parameter.

h

Table 5-77   Global Telnet SSH Parameters

Parameter	Description
Telnet	Telnet or SSH connectivity on this access point. The default is unselected.
SSH	These protocols make debugging the access point easier, especially when the access point is unable to connect to the controller.

Global IPv6 UDP Lite

This table describes the global IPv6 UDP Lite parameters used to enable or disable an IPv6 CAPWAP UDPLite for CAPWAP AP on the Cisco Wireless LAN Controller.

h

Table 5-78   Global IPv6 UDP Lite Parameters

Parameter	Description
UDP Lite	Select this check box to globally enable IPv6 UDP Lite on APs connecting to the controller using CAPWAP v6 tunnel.
	Note IPv6 UDP Lite is not applicable to APs connected with CAPWAP v4 tunnel.

Packet RSSI Location Config Parameters

This table describes the global Packet RSSI Location Config Parameters.

Table 5-79   Packet RSSI Location Config Parameters

Parameter	Description
Enable Packet RSSI Location	Enabling this feature allows the location calculations to be based off of data packets as well as probe packets. This feature requires that access points with WSM modules are deployed.
Packet Detection RSSI Minimum (dBm)	This is the minimum level at which a data packet can be heard by the WSM modules for use in location calculations. The default values is –100 db.
	It is recommended that this value be increased if you want to have only strong signals used in calculating locations.
Scan Count Threshold for Idle Client Detection (dBm)	The Scan Count Threshold represent the number of off-channel scan cycles the AP will wait before sending a Block Acknowledgment Request (BAR) to idle clients. The default value of 10 corresponds to approximately 40s, depending on the number of channels in the off channel scan cycle.
NTP Server	This is the IPv4/IPv6 address of the NTP server that all AP that are involved in this calculation need to sync to.
	It is recommended to use the same NTP server as is used by the general WLC infrastructure. The scans from multiple AP needs to be synced up for the location to be accurately calculated. An IPv4 address is required.
	Note IPv6 address is not supported.

Wireless > Advanced

Load Balancing

Choose **Wireless > Advanced > Load Balancing** to navigate to the Load Balancing page. This page enables you to configure load balancing on the wireless network.

Important Guidelines and Limitations

- Load balancing is configurable only on a per-WLAN basis.
- Load balancing is not supported on the Cisco OEAP 600 Series access point.

This table describes the load balancing parameters.

Table 5-80   Load Balancing Parameters

Parameter	Description
Client Window Size	Threshold that you can set for the client window size. This parameter specifies the threshold for the difference between the number of clients that an access point can have and the client count of the access point that has a minimum number of associated clients.
	For example, suppose in a network setup there are three access points connected to a controller (AP1, AP2, and AP3). AP1 has 2 clients, AP2 has 3 and AP3 has 4 clients. In this setup, AP1 has a minimum number of clients, that is, 2. If the window size is configured as 2, every AP can have 2 + 2 = 4 clients. So every 5th client is load balanced. If any client tries to join AP3, a denial response is sent from AP3. For a client, the denial message is sent based on the configured value for the maximum denial count.
	The default is 5.
Maximum Denial Count	Maximum denial count that you can configure. The maximum denial count specifies the maximum number of association rejections that the access point can send to a client for a given sequence of association.
	When a client tries to associate on a wireless network, it sends an association request to the access point. If the access point is overloaded and load balancing is enabled on the controller, the access point sends a denial to the association request. If there are no other access points in the range of the client, the client tries to associate the same access point again.
	After the maximum denial count is reached, the client is able to associate. Association attempts on an access point from any client before associating any AP is called a sequence of association.
	The default is 3.
Load Balancing Statistics	
Total Denial Client Count	Total number of clients denied.
Total Denial Messages Sent	Total number of denial messages sent.
Exceeded Denial Max Limit Count	Total number of messages that exceeded the denial maximum limit count.

Table 5-80   Load Balancing Parameters

Parameter	Description
None 5G Candidate Count	Number of times at the 5G band that there is no AP candidate to load balance off a client.
None 2.4 G Candidate Count	Number of times at the 2.4G band that there is no AP candidate to load balance off a client.

Band Select

Choose **Wireless > Advanced > Band Select** to navigate to the Band Select page. This page enables you to configure the band select parameters on the wireless network.

Note   Band select is not supported on the Cisco OEAP 600 Series access point.

This table describes the band select parameters.

Table 5-81   Band Select Parameters

Parameter	Description
Probe Cycle Count	Probe cycle count that you can specify.
	When a client cycle count is reached and if a client still sends a probe request, the access point responds to it with a probe response.
	For example, we assume at a minimum that a client stays in a channel for 5 milliseconds and there are 11 channels. If the client scans channel 1 and then the other 10 channels, there should be at least a gap of 10x5 milliseconds between the last time the AP hears the client probe and the latest one. The AP only increments the count if the difference of time between the latest and the last probe is more than 50 milliseconds.
	The default is 2.
Scan Cycle Period Threshold (milliseconds)	Threshold for a new scanning cycle period (in milliseconds) that you can specify.
	The Client cycle counter is incremented only if the client scans the same channel after any time the value is set for the scan cycle period threshold.
	For example, if a client is scanning a channel after every 150 milliseconds and a cycle threshold value is configured as 200, the cycle count is incremented after 300 seconds. If the client is scanning after every 250 milliseconds, the cycle count is incremented after 250 milliseconds.
	The default is 200.

Table 5-81   *Band Select Parameters (continued)*

Parameter	Description
Age Out Suppression (seconds)	Ageout suppression (in seconds) that you can configure. This parameter specifies the ageout period after which the entry of the client is removed from the suppression table.
	All entries stay in the suppression table until they are aged out or are replaced when the table is full. If the table is full, and there is no space for a new client, then the access point replaces the oldest entry on the table that had responded already. If there is no empty slot in the table, the access point has to respond to all the new clients until space is available.
	The default is 20.

Table 5-81   Band Select Parameters (continued)

Parameter	Description
Age Out Dual Band (seconds)	Ageout dual band (in seconds) that you can specify.
	When an access point receives a probe request from any client in both 2.4-GHz and 5-GHz bands, the access point is aware that the client is capable of operating on both bands. Dual-band capable clients are recorded in a dual-band client table.
	The controller keeps a record of the clients' capabilities to join the 2.4-GHz and 5-GHz bands. The controller ensures that 5-GHz capable clients join the 5-GHz band only. Entries in the table are aged out to make space for new entries. This parameter specifies the time duration after which the client entry is removed. The access point does not respond to the dual band client's 2.4-GHz probe until it is removed from the dual-band client table. The access point fills the dual-band table in the following order until it is full:
	• Clients with a 5-GHz probe that have associated to 2.4-GHz.
	• Clients with a 5-GHz probe that also have 2.4-GHz probes.
	• Clients with just a 5-GHz probe detected and a 5-GHz association.
	The default is 60.
Acceptable Client RSSI (dBm)	Acceptable client RSSI (in dBm) that you can set. This parameter specifies the minimum client RSSI threshold.
	This parameter filters out far away clients with low signal strength to limit the number of clients on the table.
	The default is –80.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Preferred Calls

You can configure a controller to support calls from clients that do not support TSPEC-based calls. This is known as voice prioritization. These calls are given priority over other clients that use the voice pool. Voice prioritization is available only for SIP-based calls, not for TSPEC-based calls. If the bandwidth is available, the controller takes the normal flow and allocates the bandwidth to those calls.

You can configure up to six preferred call numbers. When a call comes to one of the configured preferred numbers, the controller does not check on the maximum call limit. It invokes the CAC to allocate bandwidth for the preferred call. The bandwidth allocation is 85 percent of the entire bandwidth pool, not just from the maximum configured voice pool. The bandwidth allocation is the same even for roaming calls.

Prerequisites for Voice Prioritization

- WLAN QoS should be set to platinum.
- ACM should be enabled for the radio.
- WLAN should have SIP call snooping enabled.

Note   The Cisco 5500 Series Controllers and all nonmesh access points do not support the voice prioritization.

Choose **Wireless > Advanced> Preferred Calls** to navigate to this page. This page enables you to configure voice prioritization parameters on the wireless network.

Click **Add Number** to add a preferred call number.

This table describes the preferred calls parameters.

Table 5-82   Preferred Calls Parameters

Parameter	Description
Call Index	Index to assign to this call number.
Call Number	Call number.

The configured **Call Index** and **Call Numbers** are displayed.

Click **Apply** to add the index and the call number.

Click **Cancel** to return to the Preferred Calls page.

SIP Snooping

Choose **WIRELESS > Advanced > SIP Snooping** to navigate to the SIP Snooping page. This page enables you to configure call snooping ports on the controller. If you need only a single port for call snooping, configure the start and end port with the same number.

The port used by the CIUS tablet is 5060 and the port range used by Facetime is from 16384 to 16402.

This table describes the SIP snooping parameters.

Table 5-83   SIP Snooping Parameters

Parameter	Description
Port Start	Starting port for call snooping. The range is from 0 to 65535.
Port End	Ending port for call snooping. The range is from 0 to 65535.

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.

Choose **WIRELESS > Advanced > Rx SOP Threshold** to navigate to the Rx SOP Threshold page. This page enables you to configure the Rx SOP threshold values for each 802.11 band.

This table shows the Rx SOP threshold values for high, medium and low levels for each 802.11 band.

802.11 Band	High Threshold	Medium Threshold	Low Threshold
5 GHz	-76 dBm	-78 dBm	-80 dBm
2.4 GHz	-79 dBm	-82 dBm	-85 dBm

Optimized Roaming

Optimized roaming resolves the problem of sticky clients that remain associated to access points that are far away and outbound clients that attempt to connect to a Wi-Fi network without having a stable connection.

This feature disassociates clients based on the RSSI of the client data packets and data rate. The client is disassociated if the RSSI alarm condition is met and the current data rate of the client is lower than the optimized roaming data rate threshold. Optimized roaming also prevents client association when the client's RSSI is low. This feature checks the RSSI of the incoming client against the RSSI threshold. You can also configure the client coverage reporting interval for a radio.

Choose **WIRELESS > Advanced > Optimized Roaming** to navigate to the Rx SOP Threshold page. This page enables you to enable optimized roaming on a radio and configure the parameters.

This table describes the optimized roaming parameters.

Table 5-84   *Optimized Roaming Parameters*

Parameter	Description
Optimized Roaming Mode	Check box that you can select to enable Optimized Roaming.

Table 5-84   Optimized Roaming Parameters

Parameter	Description
Optimized Roaming Interval	Client coverage reporting interval for 802.11a/b networks. The range is from 5 to 90 seconds. The default value is 90.
	Note You must disable the 802.11a/b network before you configure the optimized roaming interval.
Optimized Roaming Data Rate Threshold	Threshold data rate for 802.11a/b networks.
	For 802.11a, the configurable data rates are 6, 9,12,18, 24, 36, 48, and 54.
	For 802.11b, the configurable data rates are 1, 2, 5.5, 11, 6, 9,12,18, 24, 36, 48, and 54.
	You can also choose the Disable option to disable the data rate for disassociating clients.

Network Profile

Choose **WIRELESS > Advanced > Network Profile** to navigate to the Network Profile page.

Table 5-85   Network Profile Parameters

Parameter	Description
RF Parameter Optimization	Check box that you can select to enable configuration of Client Density and Traffic Type.
Client Density	Options: • Low • Typical • High
Traffic Type	To configure RF parameters for RF traffic type such as: • Data • Data and Voice

Mesh

Choose **WIRELESS > Mesh** to navigate to the Mesh page.

This page enables you to configure the access point to establish a connection with the controller.

General

This table describes the general mesh parameters.

Table 5-86   General Parameters

Parameter	Description
Range (Root AP to Mesh AP)	Optimum distance (in feet) that should exist between the root access point and the mesh access point. This global parameter applies to all access points when they join the controller and all existing access points in the network. Values are from 150 to 132000; the default is 12,000.
IDS (Rogue and Signature Detection)	Outdoor mesh access points that you can enable or disable. The default is disable. **Note** IDS reporting is enabled for all indoor mesh access points and cannot be disabled. When you enable this feature, IDS reports are generated for all traffic on the backhaul. These reports can be useful for university or enterprise outdoor campus areas, or for public safety users who want to find out who is operating in 4.9 GHz. When you disable this feature, no IDS reports are generated, which preserves bandwidth on the backhaul.
Backhaul Client Access	Backhaul client access that you can enable or disable. The default is disable. When you enable this feature, 1520 series (152x) mesh access points allow wireless client association over the 802.11a radio, which implies that a 152x mesh access point can carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio. When you disable this feature, the 152x carries backhaul traffic over the 802.11a radio and allows client association only over the 802.11b/g radio. **Note** After you enable this feature, all mesh access points reboot.
Mesh DCA Channels	Mesh DCA channel that you can enable or disable. The default is disable. Enable this option to enable backhaul channel deselection on the controller using the DCA channel list. Any change to the channels in the controller DCA list is pushed to the associated access points. This option is only applicable for Serial Backhaul mesh access points.
Global Public Safety	Public safety band that you can enable or disable on the mesh access point.

Ethernet Bridging

This table describes the Ethernet bridging parameters.

Table 5-87   Ethernet Bridging Parameters

Parameter	Description
VLAN Transparent	VLAN transplant that you can enable or disable. This default is disable.
	When you enable this option, VLAN tags are not handled and packets are bridged as if they are untagged.
	You should disable this option if you want to enable VLAN-aware Ethernet bridging.

Security

This table describes the security parameters.

Table 5-88   Security Parameters

Parameter	Description
Security Mode	EAP (Extensible Authentication Protocol) or PSK (Preshared Key); the default option is EAP. **Note** If you enable the External MAC Filter Authorization option, you need to choose the **EAP** option. **Note** If you do not enable the External MAC Filter Authorization option, local EAP or PSK authentication is performed within the controller.

External MAC Filter Authorization	Authorization that you can enable or disable. The default is disable.
	
	Enable this option to allow an external RADIUS server to perform MAC filter authorization.
	
	This option protects your network against rogue mesh access points by preventing access points that are not defined on the external server from joining.
	
	When you enable this option and click **Apply**, the access points reboot and then rejoin the controller if defined in the MAC filter list. Access points that are not defined in the MAC list cannot join the controller.
	
	Note When this option is not enabled, by default, the controller authorizes and authenticates mesh access points using the MAC address filter.
	
	Before you employ external authentication within the mesh network, you must perform the following configuration:
	
	• On the controller, configure the RADUIS server to be used as an AAA server.
	
	• Configure the controller on the RADIUS server.
	
	• Add the mesh access point configured for external authorization and authentication to the user list of the RADIUS server.
	
	  – For remote authorization and authentication, EAP-FAST uses the manufacturer's certificate (CERT) to authenticate the child mesh access point. Additionally, this manufacturer certificate-based identity serves as the username for the mesh access point in user validation.
	
	  – For Cisco IOS-based mesh access points (1240, 1522, 1524), the platform name of the mesh access point is located in front of its Ethernet address within the certificate; therefore, the username for external RADIUS servers is *platform_name_string–Ethernet_MAC_address* such as c1240-001122334455.
	
	• Install the certificates and configure EAP-FAST on the RADIUS server.

Table 5-88   *Security Parameters*

Parameter	Description
Force External Authentication	Force external authentication that you can enable or disable. The default is disable.
	Enable this option with EAP and External MAC Filter Authorization to allow external authorization and authentication of mesh access points using a RADIUS server.
RADIUS Server	
Server Index	RADIUS server index. The Cisco WLC tries Index 1 first, then Index 2, and so on, in an ascending order. This value should be 1 if your network is using only one authentication server.
	Click the index number to display the Updating RADIUS Authentication Servers page.
Server Address	IP address of the RADIUS server.
Port	Communication port number for the interface protocols. The default is 1812.
Enabled	RADIUS authentication server that you can enable or disable.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

RF Profiles

Choose **WIRELESS > RF Profiles** to navigate to the RF Profiles page. This page enables you to create and configure RF profiles in the controller.

Out of Box AP Group

You can select the **Enable Out Of Box** check box to create an Out of Box AP group that consists of newly installed access points that belong to the default AP group. When you enable this feature:

- Newly installed access points that are part of the default AP group will be part of the Out-of-Box AP group and their radios will be switched off. This eliminates any RF instability caused by the new access points.
- All access points that do not have a group name become part of the Out of Box AP group.
- Special RF profiles are created per 802.11 band. These RF profiles have default-settings for all the existing RF parameters and additional new configurations.

When you disable this feature after you enable it, only subscription of new APs to the Out of Box AP group stops. All APs that are subscribed to the Out of Box AP Group remain in this AP group. The network administrators can move such APs to the default-group or a custom AP group upon network convergence.

Click **New** to create a new RF profile.

This table describes the RF profile parameters.

Table 5-89   RF Profile Parameters

Parameter	Description
General Parameters	
Profile Name	Name of the RF profile.
Radio Policy	Whether the RF profile will be applied to the 802.11a or 802.11b/g radios.
	Note According to the selection of the Radio Policy, the other parameters may differ.
Description	Description of the RF profile.
802.11	
Data Rates	Data rate that is Mandatory indicates that the clients that do not support this specific rate will not be able to associate with the AP.
	Data rate that is Supported indicates that any associated client that also supports this rate can communicate with the AP using this rate.
	Data rate that is Disabled indicates that clients do not support this specific rate.
	The following data rates are supported by 802.11a:
	• 6 Mbps
	• 9 Mbps
	• 12 Mbps
	• 18 Mbps
	• 24 Mbps
	• 36 Mbps
	• 48 Mbps
	• 54 Mbps
	The following data rates are supported by 802.11b/g:
	• 1 Mbps
	• 2 Mbps
	• 5.5 Mbps
	• 6 Mbps
	• 9 Mbps
	• 11 Mbps
	• 12 Mbps
	• 18 Mbps
	• 24 Mbps
	• 36 Mbps
	• 48 Mbps
	• 54 Mbps

Table 5-89   RF Profile Parameters

Parameter	Description
MCS Settings	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.
RRM > Transmit Power Control (TPC) Parameters	
Maximum Power Level Assignment	Maximum transmit power used by the RRM. The range is from –10 to 30 dBm. The default value is 30 dBm.
Minimum Power Level Assignment	Minimum transmit power used by the RRM. The range is from –10 to 30 dBm. The default value is –10 dBm.
Power Threshold v1	Transmit Power Control v1 threshold value. The range is from –80 to –50 dBm. The default value is –70 dBm. Power Threshold is the cutoff signal level used by the RRM when determining whether to reduce an access point's power.
Power Threshold v2	Configures the Transmit Power Control v2 threshold value. The range is from –80 to –50 dBm. The default value is –67 dBm.
RRM > Coverage Hole Detection Parameters	

Table 5-89   RF Profile Parameters

Parameter	Description
Data RSSI	Minimum receive signal strength indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. The range is from –60 to –90 dBm. The default value is –80 dBm.
	If the access point receives a packet in the data queue with an RSSI value below the value that you enter, it indicates that a potential coverage hole has been detected. The access point takes data RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
Voice RSSI	Minimum receive signal strength indication (RSSI) value for voice packets received by the access point. The value that you enter is used to identify coverage holes within your network. The range is from –60 to –90 dBm. The default value is –75 dBm.
	If the access point receives a packet in the voice queue with an RSSI value below the value that you enter, it indicates that a potential coverage hole has been detected. The access point takes voice RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
Coverage Exception	Minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold to trigger a coverage hole exception.
	The range is from 1 to 75, and the default value is 3.
Coverage Level	Percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. If an access point has more number of such clients than the configured coverage level it triggers a coverage hole event.
	The range is from 0 to 100%, and the default value is 25%.
	The controller determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.
RRM > DCA	
Avoid AP Foreign AP Interference	Select the **Avoid Foreign AP Interference** check box to cause the Cisco WLC's RRM algorithms to consider 802.11 traffic from foreign access points (those not included in your wireless network) when assigning channels to lightweight access points, or unselect it to disable this feature.
Channel Width	Select the required bandwidth for the AP based on the type of clients available in the RF environment.
RRM > DCA Channel List	

Table 5-89   RF Profile Parameters

Parameter	Description
DCA Channels	The DCA Channels text box shows the channels that are currently selected. To choose a channel, select its check box in the Select column. To exclude a channel, unselect its check box.
	The ranges are as follows:
	• 802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153,157, 161, 165, 190, 196
	• 802.11b/g—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
	The defaults are as follows:
	• 802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153,157, 161
	• 802.11b/g—1, 6, 11
Extended UNII-2 channels	100, 104, 108, 112, 116,132, 136, and 140—These extended UNII-2 channels in the 802.11a band do not appear in the channel list.
	If you have Cisco Aironet 1520 series mesh access points in the -E regulatory domain, you must include these channels in the DCA channel list before you start operation.
	If you are upgrading from a previous release, verify that these channels are included in the DCA channel list.
	To include these channels in the channel list, select the **Extended UNII-2 Channels** check box.
RRM > Profile Threshold For Traps	
Interference (0 to 100%)	Interference threshold on the RF environment.
Clients (1 to 200)	Number of clients present in the RF profile for which the trap is configured.
Noise (-127 to 0 dBm)	The channel noise level for trap generation.
Utilization (0 to 100 %)	The channel utilization for trap generation.
High Density and Multicast Parameters	
Maximum Clients	Maximum number of clients that can communicate with the AP in a high-density environment. The range is from 1 to 200. The default value is 200.
Client Trap Threshold	Threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller and Cisco Prime Infrastructure. The range is from 0 to 200. The default value is 50.
	Traps are disabled if the threshold value is configured as zero. Client trap threshold value should be less than then maximum clients configuration.

Table 5-89   RF Profile Parameters

Parameter	Description
Multicast Data Rates	Multicast data rate of a client with the AP.
	The following multicast data rates are supported by 802.11a and 802.11b/g:
	• 6 Mbps
	• 9 Mbps
	• 12 Mbps
	• 18 Mbps
	• 24 Mbps
	• 36 Mbps
	• 48 Mbps
	• 54 Mbps
	If you choose **auto**, the AP automatically adjusts the data rate with the client.
Rx Sop Threshold	Drop-down list from which you can choose the high, medium, or low Rx SOP threshold value for a band. For more details, see Rx SOP Threshold.
Client Distribution > Load Balancing	
Window	The window size is part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:
	load-balancing window + client associations on AP with lightest load = load-balancing threshold
	The range is from 0to 20. The default value is 5.
	In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client window size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.
Denial	The denial count sets the maximum number of association denials during load balancing. Enter a value between 1 and 10. The default value is 3.
Client Distribution > Band Select	
Note Band Select configurations are available only for 802.11BG RF profiles.	
Probe Response	Probe responses to clients that you can enable or disable.
Cycle Count	Probe cycle count for the RF profile. The cycle count sets the number of suppression cycles for a new client. The range is from 1 to 10. The default value is 2.

Table 5-89   RF Profile Parameters

Parameter	Description
Cycle Threshold	Time threshold for a new scanning RF Profile band select cycle period. This setting determines the time threshold during which new probe requests from a client come in a new scanning cycle. The range is from 1 to 1000 milliseconds. The default value is 200.
Suppression Expire	Expiration time for pruning previously known 802.11b/g clients. After this time elapses, clients become new and are subject to probe response suppression. The range is from 10 to 200 seconds. The default value is 20 seconds.
Dual Band Expire	Expiration time for pruning previously known dual-band clients. After this time elapses, clients become new and are subject to probe response suppression. The range is from 10 to 300. The default value is 60 seconds.
Client RSSI	Minimum RSSI for a client to respond to a probe. The range is from –90 to –20 dBm. The default value is –80 dBm.

Note   Changing the data rates and minimum client count requires explicit network dependencies. You must disable the 802.11a or 802.11b/g network before changing data rates and minimum client count in RF Profiles.

Click **Apply** to send the RF Profile configuration data to the Cisco WLC.

FlexConnect Groups

Choose **WIRELESS > FlexConnect Groups** to navigate to the FlexConnect Groups page. This page lists any FlexConnect groups that have already been created.

All the FlexConnect access points in a group share the same FlexConnect configuration information.

If you want to delete an existing group, click the blue arrow adjacent the group and choose **Remove**.

Cisco Centralized Key Management

FlexConnect groups are required for Cisco Centralized Key Management (CCKM) fast roaming to work with FlexConnect access points. CCKM fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can take place when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another. The FlexConnect access points need to obtain the CCKM cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller.

Note   CCKM fast roaming among FlexConnect and non-FlexConnect access points is not supported.

802.1X Authentication

FlexConnect access points support 802.1X authentication. FlexConnect access points forward the client authentication request to a local (backup) RADIUS server when the access point is in standalone mode (for example, when the WAN link is down or when the access point loses connectivity to the controller).

To enable 802.1X authentication, configure backup RADIUS servers on the FlexConnect access points to authenticate the clients when the access point is in standalone mode.

In standalone mode, if the client is connected and the session timeout has expired, the client reauthenticates with the local backup RADIUS server.

Local authentication is useful when you cannot maintain the criteria that a remote office setup has a minimum bandwidth of 128 Kbps with a round trip latency of no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Local authentication reduces the latency requirements of the branch office.

Note Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode.

Local authentication is not supported in the following scenarios:

- Guest authentication cannot be done on a FlexConnect local authentication-enabled WLAN.
- RRM information is not available at the controller for the FlexConnect local authentication-enabled WLAN.
- Local RADIUS is not supported.
- Once the client has been authenticated, roaming is only supported after the controller and the other FlexConnect access points in the group are updated with the client information

Note Only the **session timeout** RADIUS attribute is supported in the standalone mode. All other attributes are not supported.

Note RADIUS accounting is not supported in standalone mode.

Click **New** to add a new FlexConnect group.

Creating FlexConnect Groups

Choose **WIRELESS > FlexConnect Groups** and then click **New** to navigate to the FlexConnect Groups > New page.

This page allows you to create an FlexConnect group.

The number of FlexConnect groups and access point support depends on the platform that you are using. You can configure the following:

- Up to 100 FlexConnect groups for a Cisco 5500 Series Wireless Controller.
- Up to 1000 FlexConnect groups for a Cisco Flex 7500 Series Wireless Controller. The Cisco Flex 7500 Series Wireless Controller can accommodate up to 50 access points per group.

- Up to 2000 FlexConnect groups for a Cisco Flex 8500 Series Wireless Controller. The Cisco Flex 8500 Series Wireless Controller can accommodate up to 100 access points per group.

- Up to 20 FlexConnect groups with up to 25 access points per group for the remaining platforms.

You can add up to 20 FlexConnect groups per controller. For the Cisco 5500 Series Wireless Controller, you can add up to 100 FlexConnect groups.

When the FlexConnect Groups > New page appears, enter the name of the new group in the Group Name text box. You can enter up to 32 alphanumeric characters.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing FlexConnect Groups

Choose **WIRELESS > FlexConnect Groups** and then click a group name to navigate to the FlexConnect Groups > Edit page.

This page enables you to configure or change the various parameters grouped under different tabs for an existing FlexConnect group. The different tabs are as follows:

- General Tab
- Local Authentication Tab
- Image Upgrade Tab
- ACL Mapping Tab
- Central DHCP Tab
- WLAN to VLAN Mapping Tab
- WLAN AVC Mapping Tab

General Tab

This table describes the FlexConnect general parameters.

Table 5-90   General Tab Parameters

Parameter	Description
Group Name	Name of the FlexConnect group.
Enable AP Local Authentication	Check box that you can select to enable local AP authentication for a FlexConnect group. The default value is unselected. The FlexConnect AP can be configured as a RADIUS server for LEAP, EAP-FAST, PEAP, or EAP-TLS client authentication.
	Note You can configure LEAP, EAP-FAST, PEAP, or EAP-TLS authentication only if AP local authentication is enabled.
FlexConnect APs	

Table 5-90   General Tab Parameters

Parameter	Description
To add an access point to the group, click **Add AP**. The Add AP area appears.	
To choose an access point that is connected to this controller, select the **Select APs from Current Controller** check box and then choose the name of the desired access point from the **AP Name** drop-down list.	
Note If you choose an access point on this controller, the MAC address of the access point is automatically entered in the Ethernet MAC field to prevent any mismatches from occurring.	
To choose an access point that is connected to a different controller, leave the **Select APs from Current Controller** check box unselected and then enter its MAC address in the **Ethernet MAC** text box.	
Note If the FlexConnect access points within a group are connected to different controllers, all controllers must belong to the same mobility group.	
Click **Add** to add the access point to this FlexConnect group. The access point's MAC address and name appear at the bottom of the page.	
AAA	AAA parameters.
Server IP Address	IP address of the primary or secondary RADIUS server.
	Note IPv6 is not supported for local authentication.
Server Type	Drop-down list from which you can choose a primary or secondary RADIUS server. See the RADIUS Authentication Servers topic for more details.
Shared Secret	RADIUS server login shared secret.
Port Number	Communication port number for the interface protocols. The default port number is 1812.
	Note Do not assign the port number that is used by another application. Use the default port or any other port unused by any other application.

Click **Add** to add the RADIUS server to the list of RADIUS servers.

Local Authentication Tab

This table describes the local authentication parameters.

Table 5-91   Local Authentication Tab Parameters

Parameter	Description
Local Users Tab	
No of Users	Number of users currently associated.
User Name	Supported local users.

Table 5-91   Local Authentication Tab Parameters

Parameter	Description
Add User	Users that you can add by either entering the username and password or by uploading a comma-separated values (CSV) file. **Note** You can add up to 100 users. • Upload CSV file—Select this option to upload a CSV file that contains user names and passwords. Each line of the file needs to be in the following format: *username*, *password* • File Name—Click **Browse** to browse to the CSV file. • Username—Enter the username of the client that you want to authenticate using LEAP, EAP-FAST, PEAP, or EAP-TLS. • Password—Enter the password of the client. • Confirm Password—Reenter the password of the client. • Add button—Click to add the user or upload the CSV file.
Remove All Users	Click the button to delete all local users.
Protocols Tab	
Enable LEAP Authentication	FlexConnect access point to authenticate clients using LEAP. You can configure LEAP authentication only when AP local authentication is configured.
Enable EAP Fast Authentication	FlexConnect access point to authenticate clients using EAP-FAST. You can configure EAP Fast authentication only when AP local authentication is configured.
Server Key (in hex)	PACs that you can send automatically to clients that do not have one during PAC provisioning. You can select the **Enable Auto key generation** check box to automatically generate the server key. To use manual PAC provisioning, enter the server key used to encrypt and decrypt PACs in the Server Key and Confirm Server Key fields. The key must be 32 hexadecimal characters.
Authority ID (in hex)	Authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.
Authority Info	Authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.
PAC Timeout (2 to 4095)	PAC timeout value. The default value is unselected. Enter the number of seconds for the PAC to remain viable in the text box. The range is 2 to 4095 seconds.
Enable PEAP Authentication	FlexConnect access point to authenticate clients using PEAP. You can configure PEAP authentication only when AP local authentication is configured.

Table 5-91   Local Authentication Tab Parameters

Parameter	Description
Enable EAP-TLS Authentication	FlexConnect access point to authenticate clients using EAP-TLS. You can configure EAP-TLS authentication only when AP local authentication is configured.
EAP TLS Certificate Download	Check box that you can select to download the EAP root and device certificate to the access point.

Image Upgrade Tab

This table describes the image upgrade parameters.

Table 5-92   Image Upgrade Tab Parameters

Parameter	Description
FlexConnect AP Upgrade	FlexConnect AP upgrade that you can enable.
Slave Maximum Retry Count	Maximum number of retries for the preimage download. This option is available if the FlexConnect AP Upgrade option is enabled.
Upgrade Image	Drop-down list from which you can choose to download the primary image, store the image as backup, or abort the download. The available options are: • Primary—Upgrades the primary image of the controller. • Backup—Upgrades the backup image of the controller. • Abort—Aborts the image upgrade. Click the **FlexConnect Upgrade** button to upgrade the image of the FlexConnect AP.
FlexConnect Master APs	
AP Name	Access point name.
Add Master	Adds a master FlexConnect AP. The following parameters are available: • Master AP Name • AP Model • Manual

ACL Mapping Tab

This tab consists of the following three tabs:

- AAA VLAN-ACL Mapping Tab
- WLAN-ACL Mapping Tab
- Policies Tab

AAA VLAN-ACL Mapping Tab

This table describes the AAA VLAN-ACL mapping tab parameters.

Table 5-93   AAA VLAN-ACL Mapping Tab Parameters

Parameter	Description
VLAN Id	ID of the VLAN for which mapping has to be done.
Ingress ACL	Drop-down list from which you can choose the ingress ACL.
Egress ACL	Drop-down list from which you can choose the egress ACL.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Click **Add** to add a VLAN-ACL mapping.

WLAN-ACL Mapping Tab

This table describes the WLAN-ACL mapping parameters.

Table 5-94   WLAN-ACL Mapping Tab Parameters

Parameter	Description
Web Auth ACL Mapping	
WLAN Id	ID of the WLAN for which the mapping has to be done.
WebAuth ACL	Drop-down list from which you select the WebAuth ACL for external web authentication. Click **Add** to add the WebAuth ACL mapping.
	For more information about creating FlexConnect ACLs, see the Adding Access Control Lists topic.
	Note You can configure up to 16 WebAuth ACLs for an access point.
Local Split ACL Mapping	
WLAN ID	WLAN ID number.
Local-split ACL	Drop-down list from which you can choose the Local Split ACL to locally switch traffic in centrally switched WLANs. Click **Add** to add the local split ACL mapping.
	Local-split configuration is applied specific to a WLAN. You can also apply this configuration from a FlexConnect group or from an AP. If the local-split configuration is applied at both the FlexConnect group level and AP level, then the configuration applied at the AP level has higher priority. In other words, the FlexConnect ACL specific to the AP has higher priority.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Click **Add** to add a WLAN FlexConnect ACL mapping.

Policies Tab

This table describes the policies parameters.

Table 5-95   Policies Tab Parameters

Parameter	Description
Policy ACL	Drop-down list from which you can select a device-based Policy AC. Click **Add** to add the Policy ACL.
	For more information about creating FlexConnect ACLs, see the Adding Access Control Lists topic.
	Note You can configure up to 16 Policy ACLs that are specific to the FlexConnect group.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Click **Add** to add a Policy ACL.

Central DHCP Tab

This table describes the central DHCP tab parameters.

Table 5-96   Central DHCP Tab Parameters

Parameter	Description
WLAN ID	ID of the WLAN.

WLAN to VLAN Mapping Tab

Until controller Release 7.4, WLAN to VLAN mapping was done per AP. From controller Release 7.5, you can map WLAN to VLAN from the FlexConnect groups. WLAN to VLAN mapping is configured on all the APs in the FlexConnect group and does not override the WLAN to VLAN mapping done on the access points. The order of priority for WLAN to VLAN mappings is highest for AP groups > FlexConnect group > WLAN.

In Release 8.1 VLAN Support/Native VLAN on FlexConnect Group feature is available, which enables you to configure VLAN Support and Native VLAN ID on a FlexConnect Group.

This table describes the WLAN to VLAN mapping parameters.

Table 5-97   WLAN to VLAN Mapping Tab Parameters

Parameter	Description
VLAN Support	Enable the VLAN Support check box and enter a Native VLAN ID.
Override Native VLAN on AP	This option overrides the VLAN Support and Native VLAN ID parameters previously configured on the Access points, changes the inheritance level at the AP to "Group-specific", removes AP Specific WLAN-VLAN Mappings and pushes the group-specific configuration including WLAN-VLAN Mapping configured on the group to all the APs in that group.
	When the override flag is set at the FlexConnect Group, modification of VLAN Support, Native VLAN ID, WLAN-VLAN Mappings and Inheritance-Level at the AP is not allowed
WLAN ID	ID of the WLAN.
Vlan Id	ID of the VLAN.

Click **Add** to add a WLAN VLAN Mapping.

WLAN AVC Mapping Tab

Table 5-98   WLAN AVC Mapping Tab Parameters

Parameter	Description
WLAN ID	ID of the WLAN.
Application Visibility	Enable the Application Visibility on the FlexConnect Group
Flex AVC Profile	Apply the FlexConnect AVC profile

FlexConnect Groups and OKC

FlexConnect Groups enable Optimistic Key Caching (OKC) to enable fast roaming of clients. OKC facilitates fast roaming by using PMK Caching in access points that are in the same FlexConnect group.

This feature prevents the need to perform a full authentication as the client roams from one access point to another. Whenever a client roams from one FlexConnect access point to another, the FlexConnect group access point calculates the PMKID using the cached PMK.

To see the PMK cache entries at the FlexConnect access point, use the **show capwap reap pmk** command. This feature is supported on Cisco FlexConnect access points.

Note   The FlexConnect access point must be in connected mode when the PMK is derived during WPA2/802.1X authentication.

FlexConnect ACLs

With FlexConnect ACLs, you can control access at the FlexConnect AP for protection and integrity of locally switched data traffic from the AP. Using the controller, you can create FlexConnect ACLs and then configure the FlexConnect ACL with the WLAN using WLAN-ACL mapping. These are then pushed to the AP.

Choose **WIRELESS > FlexConnect ACLs** to navigate to the FlexConnect ACLs page.

This page enables you to list the ACLs configured for FlexConnect access points. To remove a FlexConnect ACL, click the blue arrow adjacent the access point and choose **Remove**.

Click **New** to open the Access Control Lists > New page.

Adding FlexConnect ACLs

Choose **WIRELESS > FlexConnect ACLs** and click **New**. This page enables you to create an ACL. Enter the FlexConnect ACL name in the Access Control List Name text box.

Click **Apply** to create a new FlexConnect ACL with the configured name.

Editing Access Control List

Choose **WIRELESS > FlexConnect ACLs** and click the ACL name of an existing ACL to open the Access Control List > Edit page.

This table describes the FlexConnect ACL parameters.

Table 5-99   FlexConnect Access Control List Parameters

Parameter	Description
General	
Access List Name	Name of the FlexConnect ACL.
Seq	Up to 64 rules can be defined for each ACL.
	The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5.
	Note If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 6 to 7 and sequence 5 to 6.
Action	Deny or Permit.
	Note The default filter is to deny all access unless a rule explicitly permits it.
Source IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.

Table 5-99   FlexConnect Access Control List Parameters

Parameter	Description
Destination IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Protocol	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol (For IPv4 ACL) • ICMPv6-Internet Control Message Protocol (For IPv6 ACL) • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA Website)
Source Port	Any or IP address and netmask.
Dest Port	Any or IP address and netmask.
DSCP	Any or Specific (from 0 to 63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service (QoS) across the Internet.

Click **Add a New Rule** to add a new rule to an existing ACL.

Adding FlexConnect ACL Rules

Choose **SECURITY > Access Control List > FlexConnect ACLs** to navigate to the FlexConnect Access Control Lists page. Click an ACL name of an existing ACL to open the **Access Control List > Edit** page and click **Add New Rule** button to create a new ACL Rule.

This table describes the FlexConnect New ACL parameters.

Table 5-100   FlexConnect ACL New Rule Parameters

Parameter	Description
Sequence	Operator that can define up to 64 rules for each ACL.
	The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is be added as rule 5.
	Note If you add or change a sequence number, the Operating System adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the Operating System automatically reassigns sequence 6 to 7 and Sequence 5 to 6.
Source	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Destination	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Protocol **Note** When you select some of these protocols, one or more additional data entry fields open up. Enter the port number in a single data entry field, or enter the source and destination port when there are two data entry fields.	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol (For IPv4 ACL) • ICMPv6-Internet Control Message Protocol (For IPv6 ACL) • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA's Website)

Table 5-100   FlexConnect ACL New Rule Parameters

Parameter	Description
DSCP	Any or Specific (from 0–63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.

802.11a/n/ac Global Parameters

Choose **WIRELESS > 802.11a/n/ac > Global Parameters** to navigate to the 802.11a/n/ac Global Parameters page. This page enables you to change the global parameters of your 802.11a/n network.

This table describes the 802.11a/n global parameters.

Table 5-101   802.11a/n Global Parameters

Parameter	Description
802.11a Network Status	802.11a/n network status. **Note** You must enable this option to enable the 802.11a/n network after configuring other 802.11a/n parameters. This option enables only the global Cisco WLAN Solution 802.11a/n network. To disable the 802.11a, 802.11b, 802.11g, and/or 802.11n networks for an individual WLAN, see the Editing WLANs page.
Beacon Period	Rate (in milliseconds) at which the SSID is broadcast by the access point. Valid values are from 100 to 600; the default is 100.
Fragmentation Threshold	Fragmentation threshold that you can set. Valid values are from 256 to 2346 bytes; the default is 2346.
DTPC Support	DTPC support. Enable this option to advertise the transmit power level of the radio in the beacons and the probe responses.
Maximum Allowed Clients	Maximum clients allowed per radio.
RSSI Low Check	Check box that you can enable to reject a client association request if the Received Signal Strength Indicator (RSSI) is lower than the configured RSSI threshold.
RSSI Threshold	RSSI Threshold that is used to reject the client association request. The range is from –60 to –90 dBm. The default value is –80 dBm.
802.11a Band Status	802.11a/n low-band, mid-band, and high-band statuses.

Table 5-101   802.11a/n Global Parameters

Parameter	Description
Data Rates	Data rates that are negotiated here are negotiated between the client and the Cisco WLC. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Cisco WLC, the client may negotiate for the respective rate. Each data rate can also be set to Disabled to match client settings.
CCX Location Measurement	Mode that enables CAPWAP access points to issue broadcast Radio Measurement Request messages to Cisco Compatible Extensions (V2 and higher) clients. This Measurement Request message is repeated periodically for every SSID over each enabled radio interface based on the specified interval. The response from the client is used to improve accuracy in location measurement.
	Interval (seconds)—Interval of the broadcast Radio Measurement Request messages.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11a/n/ac RF Grouping

Choose **WIRELESS > 802.11a/n/ac > RRM > RF Grouping** to navigate to the RF Groupingpage.

This page enables you to edit the RF grouping characteristics.

This table describes the RF grouping algorithm parameters.

Table 5-102   RF Grouping Algorithm Parameters

Parameter	Description
Group Mode	RF grouping that can be configured in any of these modes: • **leader** **Note** IPv6 is supported for RF grouping in static-leader mode. • **auto** **Note** IPv6 is not supported for RF grouping in auto mode. It supports only IPv4. • **off**. When the group mode is off, no RF grouping occurs. When a controller reboots, it starts by being a standalone leader to itself. In auto mode, the controllers form an RF group and elect an auto leader (group mode is auto mode) if the neighboring APs are in the same RF domain. In static mode, the user can configure the static leader by selecting the leader from the group mode drop-down list. The members' management IP addresses and system name are used to request the member to join the static-leader. **Note** A static leader is not allowed to become a member of another controller until its mode is **auto**. **Note** A controller with a lower priority cannot assume the role of a group leader if a controller with a higher priority is available in the RF group. Click **Restart** to restart the RRM RF grouping.
Group Role	Current role of the controller.
Group Update Interval	Interval (in seconds) that represents the period with which the grouping algorithm is run by the group leader. The Grouping algorithm also runs when the group contents change and automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. This value is set at 600 seconds.

Table 5-102   RF Grouping Algorithm Parameters

Parameter	Description
Group Leader	Name and IPv4/IPv6 address of the group leader for the group that contains the Cisco WLC.
	The RF Group Leader can be configured in two ways, as follows:
	• Auto Mode—In this mode, the members of an RF group elect an RF group leader to maintain a "master" power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or if RF group members experience major changes).
	• Static Mode—In this mode, the user selects a controller as an RF Group leader manually. In this mode, the leader and the members are manually configured and are therefore fixed. If the members are unable to join the RF Group, the reason is indicated. The leader tries to establish a connection with a member every 1 (one) minute if the member has not joined in the previous attempt.
Last Group Update	Elapsed time since the last group update in seconds. This parameter is only valid if this Cisco WLC is a group leader.

RF Group Members

This table describes the RF group parameters.

Table 5-103   RF Group Members

Parameter	Description
Controller Name	controller on which the RF Group is created.
IP Address (IPv4/IPv6)	IPv4/IPv6 address of the controller that belong to a RF group.
	Note IPv6 is supported only for leader type (static-leader) of RF grouping.

You can add a controller as a static group member by specifying the controller name and the management IP address. Click **Add** to add the controller as an RF group member.

When adding RF group members, the leader can allow the number of group members based on the following criteria:

• Maximum number of APs supported: The maximum limit for the number of access points in an RF group is 1000 or twice the maximum number APs licensed on the controller.

• Twenty controllers: Only 20 controllers (including the leader) can be part of an RF group if the sum of the access points of all controllers combined is less than or equal to the upper access point limit.

Note   If a controller cannot be added as a static RF group member, the reason is indicated in parentheses.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11a/n/ac Tx Power Control

Choose **WIRELESS > 802.11a/n/ac > RRM > TPC** to navigate to this page.

This page enables you to edit the transmit power control (TPC) parameters.

Tx Power-Level Assignment

The TPC algorithm balances RF power in many diverse RF environments. Automatic power control may not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions—for example, when all access points must be mounted in a central hallway, placing the access points close together, but requiring coverage out to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings apply only to access points that are attached to a controller from which they are configured. The default settings disable this feature, and you should use care when overriding TPC recommendations.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment text boxes, enter the maximum and minimum transmit power used by RRM on the Tx Power Control page. The range for these parameters is –10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

This table describes the Tx power level assignment parameters.

Table 5-104   Tx Power Level Assignment Parameters

Parameter	Description
TPC Version	Transmit Power Control version to be chosen from the following options: • Interference Optimal Mode (TPCv2)—For scenarios where voice calls are extensively used. Transmit power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there might be more frequent roaming and coverage hole incidents. • Coverage Optimal Mode (TPCv1)—(Default) Offers strong signal coverage. Power can be kept low to gain extra capacity and reduce interference.
Power Level Assignment Method	Dynamic transmit power assignment has three modes: • Automatic—(Default) The transmit power is periodically updated for all access points that permit this operation. • On Demand—The transmit power is updated when the **Invoke Power Update Now** is clicked. • Fixed—No dynamic transmit power assignments occur and values are set to their global default.

Table 5-104   Tx Power Level Assignment Parameters

Parameter	Description
Maximum Power Level Assignment (–10 to 30 dBm)	Maximum power level assignment on this radio. **Note** If you configure a maximum transmit power, RRM does not allow any access point attached to the controller to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually. The range is from –10 to 30 dBm. The default is 30.
Minimum Power Level Assignment (-10 to 30 dBm)	Minimum power level assignment on this radio. The range is from –10 to 30 dBm. The default is –10.
Power Threshold	Cutoff signal level used by RRM when determining whether to reduce an access point's power. The default value for this parameter varies depending on the TPC version you choose. For TPCv1, the default value is –70 dBm, and for TPCv2, the default value is –67 dBm. The default value can be changed when access points are transmitting at higher (or lower) than desired power levels. The range for this parameter is –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at higher transmit power levels. Decreasing the value has the opposite effect. **Note** In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm in order to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.
Power Neighbor Count	Minimum number of neighbors that an access point must have for the transmit power control algorithm to run.
Power Assignment Leader	Name and IP address of the power level assignment leader.
Last Power Level Assignment	Elapsed time since the last transmit power assignment in seconds.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11a/n/ac Dynamic Channel Assignment

Choose **WIRELESS > 802.11a/n/ac > RRM > DCA** to navigate to the Dynamic Channel Assignment page.

This page enables you to specify the channels that the dynamic channel assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning.

This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

Information About the RRM Start-Up Mode

- For a single controller setup, RRM start-up mode will take effect after a controller reboot.

- For a multicontroller setup, RRM start-up mode will take effect after RF Group leader election.

- The RRM start-up mode runs for 100 minutes (10 iterations at a 10-minute interval).

- The duration of the start-up mode is independent of the DCA interval, sensitivity, and network size.

- DCA start-up mode consists of 10 DCA runs with high sensitivity (making channel changes easy and sensitive to the environment) to converge to a steady state channel plan.

- After the start-up mode is finished, DCA continues to run at the interval and sensitivity specified by the user.

Dynamic Channel Assignment Algorithm

This table describes the DCA algorithm parameters.

Table 5-105   DCA Algorithm Parameters

Parameter	Description

Channel Assignment Method	DCA has three modes:
	
	• Automatic—Mode that periodically updates the channel assignments for all access points that permit this operation.
	
	   – Interval—How often the DCA algorithm has been configured to run.
	
	Note If your controller supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.
	
	   – Anchor Time—The time of day when the DCA algorithm has been configured to start. The range is from 0 to 23 (12:00 a.m. to 11:00 p.m.)
	
	• Freeze—Mode that causes the controller to evaluate and update the channel assignment for all joined access points, if necessary, but only when you click **Invoke Channel Update Once**.
	
	Note The controller does not evaluate and update the channel assignment immediately after you click **Invoke Channel Update Once**. It waits for the next interval to elapse.
	
	• OFF—Mode that turns off DCA and sets all access point radios to the first channel of the band, which is the default value. If you choose this option, you must manually assign channels on all radios.
	
	The default is Automatic.

Avoid Foreign AP Interference	Radio Resource Management (RRM) Foreign 802.11 interference-monitoring parameter that you can enable Radio Resource Management to consider interference from foreign (non-Cisco access point outside the RF/mobility domain) access points when assigning channels to Cisco access points. You can disable this parameter to have Radio Resource Management ignore this interference. In certain circumstances with significant interference energy (dBm) and load (utilization) from Foreign APs, Radio Resource Management may adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the Foreign APs to increase capacity and reduce variability for the Cisco WLAN Solution.

Table 5-105   DCA Algorithm Parameters

Parameter	Description
Avoid Cisco AP Load	Radio Resource Management (RRM) bandwidth-sensing parameter that you can enable or disable to have controllers consider the traffic bandwidth used by each access point when the controller assigns channels to the access points. Disable this parameter to have Radio Resource Management ignore this value. The default is enabled. In certain circumstances and with denser deployments, there may not be enough channels to properly create perfect channel reuse. In these circumstances, Radio Resource Management can assign better reuse patterns to those access points that carry more traffic load.
Avoid non-802.11a Noise	Radio Resource Management (RRM) noise-monitoring parameter that you can enable to have access points avoid the channels that have interference from nonaccess point sources, such as microwave ovens or Bluetooth devices. You can disable this parameter to have Radio Resource Management ignore this interference. The default is enabled. In circumstances with significant interference energy (dBm) from non-802.11 noise sources, Radio Resource Management may adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources to increase capacity and reduce variability.
Avoid Persistent Non-WiFi Interference	Persistent non-Wi-Fi interference devices that you can enable or disable.
Channel Assignment Leader	Name and IP address of the channel assignment leader. This is the MAC address of the group leader.
Last Auto Channel Iteration	Last time that the Radio Resource Management (RRM) evaluated the current channel assignment on a periodic basis. This parameter does not imply that channels have changed, only that the Radio Resource Management has made an evaluation of the current assignment.
DCA Channel Sensitivity	Configured DCA sensitivity setting. This setting determines how sensitive the DCA algorithm is to environmental changes, such as signal, load, noise, and interference, when determining whether to change channels. **Note** To see why the DCA algorithm changed channels, click **Monitor** and then **View All** under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

Table 5-105   DCA Algorithm Parameters

Parameter	Description
Channel Width[1]	Channel bandwidth supported for all the 802.11n/ac radios in the 5-GHz band: 20 MHz, 40 MHz, or 80 MHz.
	40-MHz channelization allows radios to achieve higher instantaneous data rates (potentially 2.25 times higher than 20-MHz channels).
	Note If you choose 40 MHz, be sure to choose at least two adjacent channels from the DCA Channel List (for example, a primary channel of 36 and an extension channel of 40). If you choose only one channel, that channel is not used for 40-MHz channel width.
	Note You cannot pair the following channels together: 116 and 112, 140 and 136, and 165 and 161.
	80 MHz channelization allows radios to achieve Very High Throughput (VHT). Adjacent 40-MHz subchannels are grouped into pairs to make 80-MHz channels.
	• If you choose 80 MHz for 802.11ac capable radios, ensure that you choose four adjacent 20-MHz channels from the DCA Channel List. You can select the primary channel and based on the available channel pairing you can configure appropriate secondary 20-MHz and 40-MHz extension channels for the radio.
Avoid check for non-DFS channel.	Check for non-DFS channels that you can enable or disable.
	DCA configuration requires at least one non-DFS channel to the list. In the EU countries, outdoor deployments do not support non-DFS channels. Customers based in EU or regions with a similar regulation must enable this option.

1. To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20-MHz, 40-MHz, or 80-MHz mode on the Configuring 802.11a/n APs page. If you change the static RF channel assignment method to Global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

DCA Channel List

This table describes the DCA channel list parameters.

Table 5-106   DCA Channel List Parameters

Parameter	Description
DCA Channels	DCA channels currently selected.
Channel list	Channel list you can choose or exclude a channel. **Note** The following extended UNII-2 channels have been removed from the channel list: 100, 104, 108, 112, 116, 132, 136, 140 If you have Cisco Aironet 1520 mesh access points in the -E domain, you must include these channels in the DCA channel list before you start operation. If you are upgrading from a previous release, verify that these channels are included in the DCA channel list. To include these channels in the channel list, enable the **Extended UNII-2 channels** option.
	The channels are as follows: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165,	The default channels are as follows: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161
4.9 GHz Channel list	Channel range 1 through 26 that you can choose or include in a channel. These channels are supported on Cisco Aironet 1520 series mesh access points. The 4.9-GHz band is for public safety client access traffic only.
Extended UNII-2 channels	Extended UNII-2 channels (100, 104, 108, 112, 116, 132, 136, 140) in the channel list that you can enable or disable. The default is unselected.
India Extended UNII-3 channels	India Extended UNII-3 channels (169 and 173) in the channel list that you can enable or disable. The default is unselected.

Event Driven RRM

This table describes the event driven RRM parameters.

Table 5-107   Event Driven RRM Parameters

Parameter	Description
EDRRM	EDRRM that you can enable or disable. Radio Resource Management (RRM) to run when a CleanAir-enabled access point detects a significant level of interference. If enabled, set the sensitivity threshold level (below) at which the RRM is invoked. The default is enabled.
Sensitivity Threshold	Configured sensitivity threshold setting at which the RRM is invoked. The available values are Low, Medium, High, or Custom. When the interference level of the access point raises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity. The default value is Medium.
Custom Sensitivity Threshold	Custom sensitivity threshold that you can enter. This field is displayed if the Sensitivity Threshold is set to custom.
Rogue Contribution	Check box to configure the Rogue Duty Cycle
Rogue Duty-Cycle	Proportion of time (in percentage) during which the interfering device was active. Valid range is 1% to 99%.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11a/n/ac Coverage Hole Detection

Choose **WIRELESS > 802.11a/n/ac > RRM > Coverage** to navigate to the Coverage page.

This page enables you to configure coverage-hole detection or to specify the Received Signal Strength Indicator (RSSI) parameters.

Coverage Parameters

This table describes the RRM coverage parameters.

Table 5-108   RRM Coverage Parameters

Parameter	Description
General	
Enable Coverage Hole Detection	Coverage Hole Detection (CHD) that you can enable or disable. The default is enabled.
Coverage Threshold	
Data RSSI (–60 to –90 dBm)	Data RSSI threshold in dBm. The default is –80.
Voice RSSI (–60 to –90 dBm)	Voice RSSI threshold in dBm. The default is –75.
Min Failed Client Count per AP (1 to 75)	Minimum number of clients on an access point with a RSSI below the coverage threshold. The default is 3.
Coverage exception level per AP (0 to 100%)	Maximum desired percentage of clients on the radio of an access point operating below the desired coverage threshold. The default is 25.

802.11a/n/ac RRM

Choose **WIRELESS > 802.11a/n/ac > RRM > General** to navigate to the General page.

This page enables you to specify general radio resource management (RRM) parameters.

Profile Thresholds For Traps

This table describes the profile threshold parameters.

Table 5-109   Profile Threshold Parameters

Parameter	Description
Interference (0 to 100%)	Foreign 802.11a/n/ac interference threshold between 0 and 100 percent. The default is 10.
Clients (1 to 75)	Client threshold between 1 and 75 clients. The default is 12.
Noise (-127 to 0 dBm)	Foreign noise threshold between –127 and 0 dBm. The default is –70.
Utilization (0 to 100%)	802.11a/n/ac RF utilization threshold between 0 and 100 percent. The default is 80.

Noise/Interference/Rogue Monitoring Channels

This table describes the Noise/Interference/Rogue monitoring channel parameters.

Table 5-110   Noise/Interference/Rogue Monitoring Channel Parameters

Parameter	Description
Channel List	Country Channels drop-down list. Choose one of the following: • All Channels—RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation. • Country Channels (default)—RRM channel scanning occurs only on the data channels in the country of operation. • DCA Channels—RRM channel scanning occurs only on the channel set used by the dynamic channel assignment algorithm, which by default includes all of the nonoverlapping channels allowed in the country of operation. However, you can use the 802.11a/n/ac Dynamic Channel Assignment page to specify the channel set to be used by DCA.

Monitor Intervals

This table describes the monitor interval parameters.

Table 5-111   Monitor Interval Parameters

Parameter	Description
Channel Scan Interval	Interval (in seconds) at which the channel scanning occurs. The default is 60. **Note** If your controller supports only OfficeExtend access points, we recommend that you set the channel scan duration to 1800 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.
Neighbor Packet Frequency	Interval (in seconds) for how frequently the neighbor packets (messages) are sent, which eventually builds the neighbor list. The default is 60. **Note** If your controller supports only OfficeExtend access points, we recommend that you set the neighbor packet frequency to 600 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.
Note The range is from 60 to 3600 seconds.	

Click **Set to Factory Default** to set all Auto RF 802.11a parameters to the factory defaults.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11a/n/ac Client Roaming

Choose **WIRELESS > 802.11a/n/ac > Client Roaming** to navigate to the Client Roaming page.

This page enables you to set seamless client roaming within subnets across access points and virtual LANs (VLANs) under Layer 2 security, and between subnets under Layer 3 security.

CCX-capable clients after association receive a list of neighboring APs, which is used by the clients for selecting the appropriate APs while roaming. This list improves the roaming time. The values for RSSI and Hysteresis are used for fine tuning the roaming behavior and neighbor list.

This table describes the 802.11a/n/ac client roaming parameters.

Table 5-112   802.11a/n/ac Client Roaming Parameters

RF Parameters	Description
Mode	Mode that you can set to either default or custom.
Note The following fields can be changed when you choose Custom mode.	
Minimum RSSI	Minimum received signal strength indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.
	The actual value is in dBm (the range is from –50 to –90; the default is –85).
Hysteresis	Signal strength of a neighboring access point to enable a client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points.
	The actual value is in dB (the range is from 3 to 20; the default is 3).
Scan Threshold	RSSI value from a client's associated access point below which the client must be able to roam to a neighboring access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.
	Actual value in dBm (the range is from –50 to –90; the default value is –72).
Transition Time	Maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold.
	The actual value is in seconds (the valid range is from 1 to 5; the default value is 5).
	Note For high-speed client roaming applications in outdoor mesh environments, we recommend a setting of 1 second.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11a/n/ac Voice Parameters

Choose **WIRELESS > 802.11a/n/ac > Media** to navigate to the Media page and click on the **Voice** tab.

This page enables you to set the parameters to adjust the voice quality over the 802.11a/n/ac link.

Guidelines

- Disable all WMM-enabled WLANs before changing voice parameters. Enable the WMM-enabled WLANs again after you have applied the voice settings.

- SIP CAC should only be used for phones that support status code of 17 and do not support TSPEC-based admission control.

- SIP CAC will be supported only if SIP snooping is enabled.

This table describes the 802.11a/n/ac voice CAC parameters.

Table 5-113   802.11a/n/ac Voice CAC Parameters

Parameters	Description
Admission Control (ACM)	Voice CAC that you can enable for this radio band. The default is disable. For more information, see the "Call Admission Control" topic.
CAC Method	CAC method to use. Use **Load Based** to enable channel-based CAC and use **Static** to enable bandwidth-based CAC. The default is load-based CAC. For more information, see the "Load-Based CAC" topic.
Max RF Bandwidth (%)	Percentage of the maximum bandwidth allocated to clients for voice applications on this radio band that you can set. Once the client reaches the value specified, the access point rejects new calls on this radio band. The default value is 75%; valid values are from 5% to 85%.
Reserved Roaming Bandwidth (%)	Percentage of maximum allocated bandwidth reserved for roaming voice clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients. The default value is 6%; valid values are from 0% to 25%.
Expedited Bandwidth	Parameter that enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. This setting is disabled by default. For more information, see the "Expedited Bandwidth Request" topic.
SIP CAC Support	SIP CAC support that you can enable. The default is disabled. **Note** To use SIP CAC, you must enable SIP snooping.

Table 5-113   802.11a/n/ac Voice CAC Parameters

Parameters	Description
Per-call SIP Bandwidth Note SIP CAC should only be used for phones that do not support TSPEC-based admission control.	
SIP Codec	Codec name that you want to use on this radio. The available options are G.711, G.729, and User Defined.
SIP Bandwidth (kbps)	Bandwidth in kilobits per second that you want to assign per SIP call on the network. This parameter can be configured only when the SIP Codec selected is User Defined. The default value is 64; valid values are from 8 to 64. Note The SIP Bandwidth (Kbps) text box is highlighted only when you select the SIP codec as user-defined. If you choose the SIP codec as G.711, the SIP Bandwidth (Kbps) text box is set to 64. If you choose the SIP codec as G.729, the SIP Bandwidth (Kbps) text box is set to 8.
SIP Voice Sample Interval (msecs)	Sample interval in milliseconds that the codec must operate. Note If SIP CAC is supported and CAC method is static, the Maximum Possible Voice Calls and Maximum Possible Roaming Reserved Calls fields are displayed.
Maximum Possible Voice Calls	Maximum possible voice calls that can be made. This option is displayed if the SIP CAC method is static.
Maximum Possible Roaming Reserved Calls	Maximum possible roaming reserved calls that can be made. This option is displayed if the SIP CAC method is static.
Traffic Streams Metrics	
Metrics Collection	TSM Metrics that you can enable or disable.

Note   SIPs are available only on the following controllers: Cisco 4400, Cisco 2504, 5500, 7500, 8500 Series Wireless Controllers and on 1240, 1130, and 11n access points.

This table describes the 802.11a/n/ac TSM parameters.

Table 5-114   802.11a/n/ac TSM Parameter

Parameters	Description
Metrics collection	TSM collection. For more information, see the "Traffic Stream Metrics" topic.

Call Admission Control

Call admission control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion.

CAC enables the client to specify how much bandwidth or shared medium time would be required to accept a new call and in turn enables the access point to determine whether it is capable of accommodating this particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

To use CAC with voice applications, follow these steps:

Step 1   Configure the WLAN for Platinum QoS.

Step 2   Enable the Wi-Fi Multimedia (WMM) protocol for the WLAN.

> **Note**   You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, CAC does not operate properly.

Unscheduled automatic power save delivery (U-APSD) is enabled automatically when WMM is enabled. U-APSD is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet.

Bandwidth-Based CAC

Bandwidth-based, or static, CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call and in turn enables the access point to determine whether it is capable of accommodating this particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

> **Note**   You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, bandwidth-based CAC does not operate properly.

Load-Based CAC

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by collocated channel interference. Load-based CAC also covers the additional bandwidth consumption results from PHY and channel impairment.

In load-based CAC, the access point periodically measures and updates the utilization of the RF channel, channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. Load-based CAC prevents oversubscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

Expedited Bandwidth Request

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specification (TSPEC) request (for example, an e911 call) to the WLAN. When the controller receives this request, the controller attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

You can apply expedited bandwidth requests to both static and load-based CAC.

Expedited bandwidth requests are disabled by default. If you configured the WLAN in such a way that it does not support CCX V5 or if you disabled expedited bandwidth requests, the controller ignores all expedited requests and processes TSPEC requests as normal TSPEC requests.

The following table provides examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.

This table describes the expedited bandwidth request parameters.

Table 5-115   Expedited Bandwidth Request Parameters

CAC Mode	Reserved bandwidth for voice calls[1]	Usage[2]	Normal TSPEC Request	TSPEC with Expedited Bandwidth Request
Static CAC	75% (default setting)	Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	Rejected
Load-based CAC		Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	If the voice traffic load is light relative to the data traffic load, then it is admitted. Otherwise, rejected

1. For the static (bandwidth-based) CAC, the voice call bandwidth usage is per access point and does not take into account co-channel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.

2. Static CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

Traffic Stream Metrics

In a Voice-over-Wireless LAN (VoWLAN) deployment, four variables can affect audio quality: packet latency, packet jitter, packet loss, and roaming time. These variables are referred to as traffic stream metrics (TSM). An administrator can isolate poor voice quality issues by studying these variables.

You can configure TSM on each radio-band (for example, all 802.11a radios). The controller saves the configuration in flash memory so that it persists across reboots. After an access point receives the configuration from the controller, it enables TSM on the specified radio band.

Note   Access points support TSM in both local and FlexConnect modes.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11a/n/ac Video Parameters

Choose **WIRELESS > 802.11a/n/ac > Media** to navigate to the Media page and click the **Video** tab.

This page enables you to set video quality parameters over the 802.11a link.

Note   Disable all WMM-enabled WLANs before changing video parameters. Re-enable the WMM-enabled WLANs after you have applied the video settings.

This table describes the 802.11a/n/ac video parameters.

Table 5-116   802.11a/n/ac Video Parameters

Parameters	Description
Admission Control (ACM)	Video CAC for this radio band that you can enable or disable. The default is unselected.
CAC Method	CAC method to use. Use **Load Based** to enable channel-based CAC and use **Static** to enable bandwidth-based CAC. The default is load-based CAC.
	For more information, see the "Bandwidth-Based CAC" and "Load-Based CAC" topics.
Max RF Bandwidth (%)	Percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band.
	The range is from 5 to 85%; however, the maximum RF bandwidth cannot exceed 85% for voice and video. The default value is 0%.
Reserved Roaming Bandwidth (%)	Percentage of maximum allocated bandwidth reserved for roaming video clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming video clients.
	The range is from 0 to 25%. The default is 0%.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11a/n/ac Media Parameters

Choose **WIRELESS > 802.11a/n/ac > Media** to navigate to the Media page and click the **Media** tab. This page enables you to set voice and video quality parameters over the 802.11a link.

This table describes the media stream multicast direct parameters.

Table 5-117   Media Stream Multicast Direct Parameters

Parameters	Description
Unicast Video Redirect	Unicast video direct that you can enable or disable for this radio. The default is enabled.
Multicast Direct Admission Control	

Table 5-117   Media Stream Multicast Direct Parameters

Parameters	Description
Maximum Media Bandwidth	Percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches a specified value, the access point rejects new calls on this radio band. The default value is 85% and the range is from 5 to 85%.
Client Minimum Phy Rate	Minimum transmission data rate in kbps at which the client can operate. If the transmission data rate is below the phy rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
Maximum Retry Percent	Percentage of maximum retries that are allowed. The default value is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
Media Stream - Multicast Direct Parameters	
Multicast Direct Enable	Multicast direct that you can enable or disable for this radio. The default is enable.
Maximum Streams per Radio	Maximum number of allowed multicast direct streams per radio. The range is from 0 to 20 or you can choose **auto**. The default is **auto**. When the value is **auto**, the controller decides the value based on the radio parameters.
Best Effort QoS Admission	Parameter that you can enable or disable to have the controller admit the media stream in the best radio queue for this radio. The default is disable.

802.11 EDCA Parameters

Choose **WIRELESS > 802.11a/n/ac or 802.11b/g/n > EDCA Parameters** to navigate to the EDCA Parameters page.

This page enables you to configure enhanced distributed channel access (EDCA) parameters. EDCA parameters are designed to provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

Note   You must disable the radio network before configuring the EDCA parameters. To disable the radio network, go to the 802.11a/n/ac Global Parameters page, unselect the **802.11a Network Status** check box, and click **Apply**.

After you configure the EDCA parameter, re-enable the radio network. To re-enable the radio network, go to the 802.11a/n/ac Global Parameters page, select the **802.11a Network Status** check box, and click **Apply**.

This table describes the EDCA general parameters.

Table 5-118   EDCA General Parameters

Parameter	Description
EDCA Profile	Options from the EDCA Profile drop-down box that you can choose: • WMM — (Default) Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network. • Spectralink Voice Priority—Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls. • Voice Optimized—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network. • Voice & Video Optimized—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network. **Note** If you deploy video services, admission control (ACM) must be disabled from the 802.11a/n/ac Video Parameters page.
Enable Low Latency MAC	MAC optimization for voice that you can choose. This feature enhances voice performance by controlling packet retransmits and aging out voice packets on lightweight access points, improving the number of voice calls serviced for each access point.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11h Global Parameters

Choose **WIRELESS > 802.11a/n/ac > DFS (802.11h)** to navigate to the 802.11h Global Parameters page. This page enables you to set 802.11h parameters.

⚠

Caution   Disable the 802.11a/n/ac network before you configure the 802.11h network.

When DFS is enabled, it detects the presence of other devices that use the same radio channel and switches the WLAN operation to another channel if necessary.

This table describes the 802.11h parameters.

Table 5-119   *802.11h Parameters*

Parameter	Description
Local Power Constraint	Local power constraint (in dBm) that you can specify. This parameter is displayed when Power Constraint is enabled. The range is from 0 to 30 dBm.
Channel Announcement	Channel announcement method in which the access point announces when it is switching to a new channel and the new channel number.
Channel Quite Mode	Channel quite mode that you can enable or disable. This parameter is displayed when Channel Announcement is enabled. The default is unselected.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11n/ac (5 GHz) Very High Throughput

Choose **WIRELESS > 802.11a/n/ac > High Throughput (802.11n/ac)** to navigate to the 802.11n/ac (5 GHz) Throughput page.

This page enables you to configure 802.11n and 802.11ac support on the network and to enable or disable support of the different modulation coding scheme (MCS) settings. The MCS settings determine the number of spatial streams, modulation, coding rate, and data rate values.

General Parameters

Disabling the 802.11n/ac mode is applicable only to access radios. Backhaul radios always have the 802.11n/ac mode enabled if they are 802.11n capable.

This table describes the 802.11a/n/ac parameters.

Table 5-120   *General Parameters*

Parameter	Description
11n Mode	The 802.11n mode that you can enable or disable on the network. The default is enabled.
	Note If you want to disable 802.11n when both 802.11n and 802.11ac are enabled, you must disable 802.11ac first.
11ac Mode	The 802.11ac mode that you can enable or disable on the network. The default is enabled.
	Note You can modify the 802.11ac status only if 802.11n is enabled.
HT MCS Index	Setting for a specific High Throughput (HT) Modulation and Coding Scheme (MCS) index value that you can enable or disable (0 through 23). Data rates are determined according to the MCS index. By default, all are selected.

Table 5-120   General Parameters

Parameter	Description
SS	Signals transmitted by the various antennae are multiplexed by using different spaces within the same spectral channel. These spaces are known as spatial streams.
	Three spatial streams are available within which you can enable or disable an MCS data rate.
VHT MCS Index (Data Rate)	Setting for a specific Very High Throughput (VHT) MCS that you can enable or disable (0 through 9). By default, all are selected.
	MCS index 8 and 9 are specific to 802.11ac. Enabling MCS data rate with index 9 automatically enables data rate with MCS index 8. You can enable or disable MCS index 8 only when MCS index 9 is disabled.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11a/n/ac CleanAir

To configure the Cisco CleanAir functionality on the 802.11a/n/ac network using the controller GUI, follow these steps:

Step 1 Choose **Wireless > 802.11a/n/ac > CleanAir** to navigate to the 802.11a/n/ac > CleanAir page.

> **Note** Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

Step 2 Select the **CleanAir** check box to enable the CleanAir functionality on the 802.11a/n/ac network, or unselect the check box to prevent the controller from detecting spectrum interference. The default is disabled.

Step 3 Select the **Report Interferers** check box to enable the CleanAir system to report any detected sources of interference, or unselect it to prevent the controller from reporting interferers. The default is enabled.

> **Note** Device Security alarms, Event Driven RRM, and Persistence Device Avoidance algorithm will not work if Report Interferers is disabled.

Step 4 Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points associated with the same controller. Persistent interferers are present at the location and interfere with the WLAN operations even if they are not detectable at all times.

Step 5   Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect multiple select text box and any that do not need to be detected appear in the Interferences to Ignore multiple select text box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interference sources are detected. The possible sources of interference include the following:

- Canopy—A canopy bridge device

- Continuous Transmitter—A continuous transmitter

- DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone

- Jammer—A jamming device

- SuperAG—An 802.11 SuperAG device

- TDD Transmitter—A time division duplex (TDD) transmitter

- Video Camera—A video camera

- WiFi Invalid Channel—A device using nonstandard Wi-Fi channels

- WiFi Inverted Channel—A device using spectrally inverted Wi-Fi signals

- WiMAX Fixed—A WiMAX fixed device (802.11a/n/ac only)

- WiMAX Mobile—A WiMAX mobile device (802.11a/n/ac only)

> **Note**   Access points associated to the controller send interference reports only for the type of interferer devices that appear in the Interferences to Detect text box. This functionality enables you to filter out a source of interference that you do not want as well as any that may be flooding the network and causing performance problems for the controller or Cisco PI. Filtering allows the system to resume normal performance levels.

Step 6   Configure CleanAir alarms as follows:

- Select the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or unselected the check box to disable this feature. The default value is selected.

- If you selected the Enable AQI Trap check box, enter a value between 1 and 100 (inclusive) in the AQI Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default is 35.

- Enter the **AQI Alarm Threshold (1 to 100)** that you want to set. An alarm is generated when the air quality falls below the configured threshold value. The default is 35. The range is from 1 to 100.

- Select the **Enable trap for Unclassified Interferences** check box to enable the traps to be generated for unclassified interferences. Cisco CleanAir can detect and monitor unclassified interferences. Unclassified interferences are interferences that are detected but do not correspond to any of the known interference types.

- Enter the **Threshold for Unclassified category trap (1 to 99)**. Enter a value between 1 and 99. The default is 20. This is the severity index threshold for an unclassified interference category.

- Select the **Enable Interference For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect the check box to it to disable this feature. The default value is selected.

- Make sure that any sources of interference that need to trigger interferer alarms appear in the Trap on These Types multiple select text box and any that do not need to trigger interferer alarms appear in the Do Not Trap on These Types text box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.

  For example, if you want the controller to send an alarm when it detects a jamming device, select the **Enable Interference Type Trap check box** and move the jamming device to the Trap on These Types multiple select box.

Step 7   The Event Driven RRM section displays the current status or the event-driven radio resource management configured on this radio:

- EDRRM—Displays the current status of the spectrum event-driven RRM.
- Sensitivity Threshold—Displays the threshold level at which the event-driven RRM is invoked.

> ✎
>
> **Note**   If you want to change the current status of event-driven RRM or the sensitivity level, click **Change Settings**. The **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page appears.

Step 8   Click **Apply** to commit your changes.

802.11b/g/n Global Parameters

Choose **WIRELESS > 802.11b/g/n > Network** to navigate to the 802.11b/g/n Global Parameters page.

This page enables you to edit the global parameters of your 802.11b/g/n network.

This table describes the 802.11 b/g/n global parameters.

Table 5-121   802.11 b/g/n Global Parameters

Parameter	Description
General Parameters	
802.11b/g Network Status	802.11b/g/n network parameters that you can enable or disable. The default is enabled.
802.11g Support	802.11g network support. Only available if 802.11b/g network is enabled. The default is enabled.
	Note You must use these commands to enable the 802.11b/g networks after configuring other 802.11b/g parameters. This command only enables the global Cisco WLAN Solution 802.11b/g networks. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual WLAN, see the Editing WLANs page.
Beacon Period (millisecs)	Rate at which the SSID is broadcast by the access point, from 100 to 600 milliseconds. The default is 100 milliseconds.

Table 5-121   802.11 b/g/n Global Parameters

Parameter	Description
Short Preamble	Short preamble that you can enable or disable. This parameter must be disabled to optimize this Cisco WLC for some clients, including SpectraLink NetLink Telephones. The default is enabled.
Fragmentation Threshold (bytes)	Fragmentation threshold (in bytes) that you can set in the range 256 to 2346 bytes. The default is 2346.
DTPC Support	DTPC support that you can enable or disable to advertise the transmit power level of the radio in the beacons and the probe responses. The default is unselected.
Maximum Allowed Clients	Maximum clients allowed per radio. The range is from 1 to 200.
CCX Location Measurement	Mode that enables CAPWAP access points to issue broadcast Radio Measurement Request messages to Cisco Compatible Extensions (V2 and higher) clients. This Measurement Request message is repeated periodically for every SSID over each enabled radio interface based on the specified interval. The response from the client is used to improve accuracy in location measurement.
	• Mode—Option that you enable if you want CAPWAP access points to issue broadcast Radio Measurement Request messages to Cisco Compatible Extensions (V2 and higher) clients. This Measurement Request message is repeated periodically for every SSID over each enabled radio interface based on the specified interval. The response from the client is used to improve accuracy in the location measurement. The default is unselected.
	• Interval (seconds)—Specifies the interval of the broadcast Radio Measurement Request messages.
	• Data Rates—The data rates set here are negotiated between the client and the Cisco WLC. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Cisco WLC, the client may negotiate for the respective rate. Each data rate can also be set to Disabled to match client settings.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11b/g/n RF Grouping

Choose **WIRELESS > 802.11b/g/n > RRM > RF Grouping** to navigate to the 802.11b > RRM > RF Grouping page.

This page enables you to configure RF grouping characteristics.

This table describes the RF grouping algorithm parameters.

Table 5-122   RF Grouping Algorithm Parameters

Parameter	Description
Group Mode	RF grouping that can be configured in any of these modes: • leader **Note** IPv6 is supported for RF grouping in static-leader mode. • auto **Note** IPv6 is not supported for RF grouping in auto mode. It supports only IPv4. • **off**. When the group mode is off, no RF grouping occurs. When a Cisco WLC reboots, it starts by being a standalone leader to itself. In auto mode, the Cisco WLCs form an RF group and elect an auto leader (group mode is auto mode) if the neighboring APs are in the same RF domain. In static mode, the user can configure the static leader by selecting the leader from the group mode drop-down list. The members' management IP addresses and system name are used to request the member to join the static-leader. **Note** A static leader is not allowed to become a member of another Cisco WLC until its mode is **auto**. **Note** A Cisco WLC with a lower priority cannot assume the role of a group leader if a Cisco WLC with a higher priority is available in the RF group. Click **Restart** to restart the RRM RF grouping.
Group Role	Current role of the Cisco WLC.
Group Update Interval	Interval (in seconds) that represent the period with which the grouping algorithm is run by the group leader. The grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. This value is set at 600 seconds.

Table 5-122   RF Grouping Algorithm Parameters

Parameter	Description
Group Leader	Name and IPv4/IPv6 address of the group leader for the group that contains the Cisco WLC.
	The RF Group Leader can be configured in two ways, as follows:
	• Auto Mode—In this mode, the members of an RF group elect an RF group leader to maintain a "master" power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or if RF group members experience major changes).
	• Static Mode—In this mode, the user selects a Cisco WLC as an RF Group leader manually. In this mode, the leader and the members are manually configured and are therefore fixed. If the members are unable to join the RF Group, the reason is indicated. The leader tries to establish a connection with a member every 1 (one) minute if the member has not joined in the previous attempt.
Last Group Update	Elapsed time since the last group update in seconds. This parameter is only valid if this Cisco WLC is a group leader.

This table describes the RF group member parameters.

Table 5-123   RF Group Member Parameters

Parameter	Description
Controller Name	controller on which the RF group is created.
IP Address (IPv4/IPv6)	IPv4/IPv6 address of the Cisco WLC that belong to a RF group.
	Note IPv6 is supported only for leader type (static-leader) of RF grouping.

You can add a Cisco WLC as a static group member by specifying the Cisco WLC name and the management IP address. Click **Add** to add the Cisco WLC as an RF group member.

When adding RF group members, the leader can allow the number of group members based on the following criteria:

• Maximum number of APs supported: The maximum limit for the number of access points in an RF group is 1000 or twice the maximum number APs licensed on the Cisco WLC.

• Twenty Cisco WLCs: Only 20 Cisco WLCs (including the leader) can be part of an RF group if the sum of the access points of all Cisco WLCs combined is less than or equal to the upper access point limit.

Note   If a Cisco WLC cannot be added as a static RF group member, the reason is indicated in parentheses.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11b Tx Power Control

Choose **WIRELESS > 802.11b/g/n > RRM > TPC** to navigate to the 802.11b > RRM > Tx Power Control page.

This page enables you to edit the transmit power control (TPC) parameters.

Tx Power Level Assignment

The TPC algorithm balances RF power in many diverse RF environments. Automatic power control may not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions—for example, when all access points must be mounted in a central hallway, placing the access points close together, but requiring coverage out to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings only apply to access points that are attached to a controller from which they are configured. The default settings disable this feature, and you should use care when overriding TPC recommendations.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment text boxes, enter the maximum and minimum transmit power used by RRM on the Tx Power Control page. The range for these parameters is –10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

This table describes the Tx power level assignment parameters.

Table 5-124   Tx Power Level Assignment Parameters

Parameter	Description
TPC Version	Transmit Power Control version to be chosen from the following options:
	• Interference Optimal Mode (TPCv2)—For scenarios where voice calls are extensively used. Transmit power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there could be frequent roaming delays and coverage hole incidents.
	• Coverage Optimal Mode (TPCv1)—(Default) Offers strong signal coverage and stability. In this mode, power can be kept low to gain extra capacity and reduce interference.
Power Level Assignment Method	Dynamic transmit power assignment has three modes:
	• Automatic—(Default) The transmit power is periodically updated for all access points that permit this operation.
	• On Demand—The transmit power is updated when **Invoke Power Update Now** is clicked.
	• Fixed—No dynamic transmit power assignments occur and values are set to their global default.

Table 5-124   Tx Power Level Assignment Parameters

Parameter	Description
Maximum Power Level Assignment (-10 to 30 dBm)	Maximum power level assignment on this radio. **Note** If you configure a maximum transmit power, RRM does not allow any access point attached to the controller to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually. The range is –10 to 30 dBm. The default is 30.
Minimum Power Level Assignment (–10 to 30 dBm)	Minimum power level assignment on this radio. The range is –10 to 30 dBm. The default is –10.
Power Assignment Leader	Name and IP address of the power level assignment leader.
Last Power Level Assignment	Elapsed time since the last transmit power assignment in seconds.
Power Threshold	Cutoff signal level used by RRM when determining whether to reduce an access point's power. The default value for this parameter varies depending on the TPC version you choose. For TPCv1, the default value is –70 dBm, and for TPCv2, the default value is –67 dBm. The default value can be changed when access points are transmitting at higher (or lower) than desired power levels. The range for this parameter is –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at higher transmit power rates. Decreasing the value has the opposite effect. **Note** In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm in order to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.
Power Neighbor Count	Minimum number of neighbors that an access point must have for the transmit power control algorithm to run.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11b Dynamic Channel Assignment

Choose **WIRELESS > 802.11b/g/n > RRM > DCA** to navigate to the 802.11b > RRM > Dynamic Channel Assignment page.

This page enables you to specify the channels that the Dynamic Channel Assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning.

This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

Dynamic Channel Assignment Algorithm

This table describes the DCA algorithm parameters.

Table 5-125   DCA Algorithm Parameters

Parameter	Description

Channel Assignment Method	Dynamic channel assignment has three modes:
	
	• Automatic—Mode that periodically updates for all access point that permit this operation.
	
	   – Interval—How often the DCA algorithm has been configured to run.
	
	Note If your controller supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.
	
	   – Anchor Time—The time of day when the DCA algorithm has been configured to start. The range is from 0 to 23 (12:00 a.m. to 11:00 p.m).
	
	• Freeze—Mode that causes the controller to update channel assignments when you click **Invoke Channel Update Now**.
	
	• OFF—Mode that turns off DCA and sets all access point radios to the first channel of the band, which is the default value. If you choose this option, you must manually assign channels on all radios.
	
	The default is Automatic.

Avoid Foreign AP Interference	Radio Resource Management (RRM) Foreign 802.11 interference-monitoring parameters that you can enable to have Radio Resource Management consider interference from foreign (non-Cisco access point outside the RF/mobility domain) access points when assigning channels to Cisco access points. You can disable this parameter to have Radio Resource Management ignore this interference. The default is unselected. In certain circumstances with significant interference energy (dBm) and load (utilization) from Foreign APs, Radio Resource Management may adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the Foreign APs to increase capacity and reduce variability.
Avoid Cisco AP Load	Radio Resource Management (RRM) Bandwidth-sensing parameter that you can enable controllers to consider the traffic bandwidth used by each access point when assigning channels to access point. You can disable this parameter to have Radio Resource Management ignore this value. The default is unselected. In certain circumstances and with denser deployments, there may not be enough channels to properly create perfect channel reuse. In these circumstances, Radio Resource Management can assign better reuse patterns to those access points that carry more traffic load.

Table 5-125   DCA Algorithm Parameters

Parameter	Description
Avoid non-802.11a Noise	Radio Resource Management (RRM) Noise-monitoring parameter that you can enable to have access points avoid channels that have interference from non-Access Point sources, such as microwave ovens or Bluetooth devices. Disable this parameter to have Radio Resource Management ignore this interference.
	In circumstances with significant interference energy (dBm) from non-802.11 noise sources, Radio Resource Management may adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources to increase capacity and reduce variability.
Avoid Persistent Non-WiFi Interference	DCA parameter that you can enable to allow the controller to ignore persistent non-WiFi interference.
Channel Assignment Leader	Name and IP address of the channel assignment leader. Cisco WLAN Solution, mobility groups Cisco WLAN Solution WPS groups. This is the MAC address of the group leader.
Last Auto Channel Assignment	Last time the Radio Resource Management (RRM) evaluated the current channel assignment on a periodic basis. This parameter does not imply that channels have changed, only that the Radio Resource Management has made an evaluation of the current assignment.
DCA Channel Sensitivity	Configured DCA sensitivity setting.
	This setting determines how sensitive the DCA algorithm is to environmental changes, such as signal, load, noise, and interference, when determining whether to change channels. The available values are as follows:
	• Low—The DCA algorithm is not particularly sensitive to environmental changes.
	• Medium—The DCA algorithm is moderately sensitive to environmental changes.
	• High—The DCA algorithm is highly sensitive to environmental changes.
	The default value is Medium. The DCA sensitivity thresholds vary by radio band.
	Note To see why the DCA algorithm changed channels, click **Monitor** and then **View All** under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

DCA Channel List

This table describes the DCA channel list parameters.

Table 5-126   DCA Channel List Parameters

Parameter	Description	
DCA Channels	Channels that are currently selected.	
Select/Channel	Select or exclude a channel.	
	Channels are as follows: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	The default channels are as follows: 1, 6, 11

Event Driven RRM

This table describes the event driven RRM parameters.

Table 5-127   Event Driven RRM Parameters

Parameter	Description
EDRRM	Radio Resource Management (RRM) that you can enable or disable to run when a CleanAir enabled access point detects a significant level of interference. The default is unselected. If enabled, set the sensitivity threshold level (below) at which the RRM is invoked.
Sensitivity Threshold	Configured sensitivity threshold setting at which the RRM is invoked. The available values are Low, Medium, High, or Custom. When the interference for the access point rises and the corresponding AQ index falls below the threshold level, RRM initiates a local channel assignment and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity. If you selected the EDRRM sensitivity threshold as custom, you must set a threshold value in the Custom Sensitivity Threshold field. The default sensitivity is 35. The EDRRM AQ threshold value for low sensitivity is 35, medium sensitivity is 50, and high sensitivity is 60. The default value is Medium.
Rogue Contribution	Check box to configure the Rogue Duty Cycle
Rogue Duty-Cycle	Proportion of time (in percentage) during which the interfering device was active. Valid range is 1% to 99%.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11b Coverage Hole Detection

Choose **WIRELESS > 802.11b/g/n > RRM > Coverage** to navigate to the 802.11b > RRM > Coverage page.

This page enables you to configure coverage-hole detection or to specify the RSSI parameters.

This table describes the RRM coverage parameters.

Table 5-128   RRM Coverage Parameters

Parameter	Description
General	
Enable Coverage Hole Detection	Coverage Hole Detection (CHD) that you can enable or disable.
Coverage Threshold	
Data RSSI (-60 to -90 dBm)	Minimum receive signal strength indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. The range is from –60 to –90 dBm. The default value is –80 dBm.
	If the access point receives a packet in the data queue with an RSSI value below the value that you enter, it indicates that a potential coverage hole has been detected. The access point takes data RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
Voice RSSI (-60 to -90 dBm)	Minimum receive signal strength indication (RSSI) value for voice packets received by the access point. The value that you enter is used to identify coverage holes within your network. The range is from –60 to –90 dBm. The default value is –75 dBm.
	If the access point receives a packet in the voice queue with an RSSI value below the value that you enter, it indicates that a potential coverage hole has been detected. The access point takes voice RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
Min Failed Client Count per AP (1 to 75)	Minimum number of clients on an access point with a signal-to-noise ratio (SNR) below the coverage threshold.
	The default value is 3.
Coverage exception level per AP (0 to 100%)	Maximum desired percentage of clients on an access point's radio operating below the desired coverage threshold.
	The default value is 25.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11b RRM

Choose **WIRELESS > 802.11b/g/n > RRM > General** to navigate to the 802.11b > RRM > General page.

This page enables you to specify general radio resource management (RRM) parameters.

> **Note**   The radios for the Cisco OEAP 600 Series access points are controlled through the local GUI on the Cisco OEAP 600 Series access points and not through the controller. It is not possible to control the spectrum channel, power, or disable the radios through the controller because it does not have any effect on the Cisco OEAP 600 Series access points. Therefore, RRM is not supported on the Cisco OEAP 600 Series access points.

This table describes the profile threshold parameters.

Table 5-129   Profile Threshold Parameters

Parameter	Description
Interference (0 to 100%)	Foreign 802.11b/g interference threshold between 0 and 100 percent. The default value is 10.
Clients (1 to 75)	Client threshold between 1 and 75 clients. The default value is 12.
Noise (-127 to 0 dBm)	Foreign noise threshold between –127 and 0 dBm. The default value is –70.
Utilization (0 to 100%)	802.11b/g RF utilization threshold between 0 and 100 percent. The default value is 80.

Noise/Interference/Rogue Monitoring Channels

This table describes the Noise/Interference/Rogue monitoring channels parameters.

Table 5-130   Noise/Interference/Rogue Monitoring Channels Parameters

Parameter	Description
Channel List	Country Channels drop-down box that you can choose one of the following: • All Channels—RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation. • Country Channels (default)—RRM channel scanning occurs only on the data channels in the country of operation. • DCA Channels—RRM channel scanning occurs only on the channel set used by the dynamic channel assignment (DCA) algorithm, which by default includes all of the nonoverlapping channels allowed in the country of operation. However, you can use the 802.11a/n/ac Dynamic Channel Assignment page to specify the channel set to be used by DCA.

Monitor Intervals

This table describes the monitor interval parameters.

Table 5-131   Monitor Interval Parameters

Parameter	Description
Channel Scan Interval	Interval (in seconds) at which the channel scanning occurs.
	The default value is 180.
	Note If your controller supports only OfficeExtend access points, We recommend that you set the channel scan duration to 1800 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.
Neighbor Packet Frequency	Interval (in seconds) for how frequently the access point measures signal strength and how frequently neighbor packets (messages) are sent, which eventually builds the neighbor list.
	The default value is 60.
	Note If your controller supports only OfficeExtend access points, We recommend that you set the neighbor packet frequency to 600 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.

Note   The valid interval range is from 60 to 3600 seconds.

Click **Set to Factory Default** to set all Auto RF 802.11b/g parameters to the factory defaults.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11b/g Client Roaming

Choose **WIRELESS > 802.11b/g > Client Roaming** to navigate to the 802.11b > Client Roaming page. Seamless client roaming within subnets across access points and virtual LANs (VLANs) is supported under Layer 2 security, and between subnets under Layer 3 security.

CCX-capable clients after association receive a list of neighboring APs, which is used by the clients for selecting the appropriate APs while roaming. This improves the roaming time. The values for RSSI and Hysteresis are used for fine tuning the roaming behavior and Neighbor list.

This table describes the 802.11b/g client roaming parameters.

Table 5-132   802.11b/g Client Roaming Parameters

RF Parameters	Description
Mode	Drop-down box: Default or Custom.

Note   The following fields can be changed when you select Custom mode.

Table 5-132   802.11b/g Client Roaming Parameters

RF Parameters	Description
Minimum RSSI	Actual value in dBm (the valid range is from –80 to –90; the default value is –85).
	This parameter indicates the minimum received signal strength indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.
Hysteresis	Actual value in dB (the valid range is from 2 to 4; the default value is 2).
	This parameter indicates how strong the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points.
Scan Threshold	Actual value in dBm (the valid range is from –70 to –77; the default value is –72).
	This parameter indicates the RSSI value, from a client's associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.
Transition Time	Actual value in seconds (the valid range is from 1 to 10; the default value is 5).
	Note For high-speed client roaming applications in outdoor mesh environments, a setting of 1 second is recommended.
	This parameter indicates the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11b/g Voice Parameters

Choose **WIRELESS > 802.11b/g > Media** to navigate to the 802.11b (2.4 GHz) > Media pageand click on the **Voice** tab.

This page enables you to set the voice quality parameters over the 802.11 b/g link.

Note   Disable all WMM-enabled WLANs prior to changing voice parameters. Reenable the WMM-enabled WLANs after you have applied the voice settings.

CAC Parameters

This table describes the 802.11b/g CAC parameters.

Table 5-133   802.11b/g CAC Parameters

Parameters	Description
Admission Control (ACM)	Voice CAC for this radio band that you can enable or disable. The default value is disabled. For more information, see the "Call Admission Control" topic.
Load-based CAC	Load-based CAC that you can enable or disable. Load-based AC is disabled by default. For more information, see the "Load-Based CAC" topic.
Max RF Bandwidth (%)	Percentage of the maximum bandwidth allocated to clients for voice applications on this radio band. Once the client reaches the value specified, the access point rejects new calls on this radio band. The default value is 75%; valid values are from 40% to 85%.
Reserved Roaming Bandwidth (%)	Percentage of maximum allocated bandwidth reserved for roaming voice clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients. The default value is 6%; valid values are from 0% to 25%.
Expedited Bandwidth	Enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. This setting is enabled by default. For more information, see the "Expedited Bandwidth Request" topic.
SIP Codec	Codec name that you want to use on this radio. The available options are G.711, G.729, and User Defined.
SIP Bandwidth (kbps)	Bandwidth in kilobits per second you want to assign per SIP call on the network. This parameter can be configured only when the SIP Codec selected is User Defined.
SIP Voice Sample Interval (msecs)	Sample interval in milliseconds that the codec must operate.

Note   SIPs are available only on the Cisco 4400 Series Controllers and the Cisco 5500 Series Controllers and on for the following access points: 1240, 1130, and 11n.

802.11 b/g TSM Parameters

This table describes the 802.11b/g TSM parameters.

Table 5-134   *802.11b/g TSM Parameters*

Parameters	Description
Metrics collection	TSM collection that you can enable or disable. The default is unselected.
	For more information, see the "Traffic Stream Metrics (TSM)" topic.

Call Admission Control

Call admission control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion.

CAC enables the client to specify how much bandwidth or shared medium time would be required to accept a new call and in turn enables the access point to determine whether it is capable of accommodating this particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

To use CAC with voice applications, do the following:

- Configure the WLAN for Platinum QoS
- Enable the Wi-Fi Multimedia (WMM) protocol for the WLAN

Note You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, CAC does not operate properly.

Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. U-APSD is enabled automatically when WMM is enabled.

Load-Based CAC

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

In load-based CAC, the access point periodically measures and updates the utilization of the RF channel, channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents over-subscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

Expedited Bandwidth Request

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. When the controller receives this request, the controller attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

You can apply expedited bandwidth requests to both static and load-based CAC.

Expedited bandwidth requests are enabled by default. If you configured the WLAN in such a way that it does not support CCX V5 or if you disabled expedited bandwidth requests, the controller ignores all expedited requests and processes TSPEC requests as normal TSPEC requests.

See the following table for examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.

This table describes the expedited bandwidth request parameters.

Table 5-135   Expedited Bandwidth Request Parameters

CAC Mode	Reserved bandwidth for voice calls[1]	Usage[2]	Normal TSPEC Request	TSPEC with Expedited Bandwidth Request
Static CAC	75% (default setting)	Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	Rejected
Load-based CAC		Less than 75%	Admitted	Admitted
		Between 75% and 85% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 85%	Rejected	Rejected

1. For the static (bandwidth-based) CAC, the voice call bandwidth usage is per access point and does not take into account co-channel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.

2. Static CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

Traffic Stream Metrics (TSM)

In a voice-over-wireless LAN (VoWLAN) deployment, four variables can affect audio quality: packet latency, packet jitter, packet loss, and roaming time. These variables are referred to as TSM. An administrator can isolate poor voice quality issues by studying these variables.

You can configure TSM on a per radio-band basis (for example, all 802.11a radios). The controller saves the configuration in flash memory so that it persists across reboots. After an access point receives the configuration from the controller, it enables TSM on the specified radio band.

Note   Access points support TSM in both local and FlexConnect modes.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11b/g/n Video Parameters

Choose **WIRELESS > 802.11b/g/n > Media** to navigate to the 802.11b(2.4 GHz) > Media page and click on the **Video** tab.

This page enables you to set the parameters to adjust video quality over an 802.11b/g/n link.

Note   Disable all WMM-enabled WLANs prior to changing video parameters. Reenable the WMM-enabled WLANs after you have applied the video settings.

This table describes the 802.11b/g video parameters.

Table 5-136   802.11b/g Video Parameters

Parameters	Description
Admission Control (ACM)	Video CAC for this radio band that you can enable or disable. The default is unselected.
Max RF Bandwidth (%)	Percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band. The valid range is from 0 to 100%; however, the maximum RF bandwidth cannot exceed 100% for voice + video. The default value is 0%.
Reserved Roaming Bandwidth (%)	Percentage of maximum allocated bandwidth reserved for roaming video clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming video clients. The valid range is from 0 to 25%. The default value is 0%.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11b/g Media Parameters

Choose **WIRELESS > 802.11b/g/n > Media** to navigate to the 802.11b(2.4 GHz) > Media page and click on the **Media** tab.

This page enables you to set the video quality parameters over an 802.11b/g/n link.

This table describes the 802.11 b/g/n general media parameters.

Table 5-137   802.11 b/g/n General Media Parameters

Parameter	Description
Unicast Video Redirect	Enables unicast video redirect. The default value is enabled.

This table describes the multicast direct admission control parameters.

Table 5-138   Multicast Direct Admission Control Parameters

Parameter	Description
Maximum Media Bandwidth (0 - 85%)	Percentage of maximum bandwidth allocated to clients for media applications on this radio band. Once the client reaches the value specified, the access point rejects new calls on this radio band. The default value is 85%; valid values are from 0 –85%.
Client Phy rate	Minimum transmission data rate to the client. If the transmission data rate is below the phy rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
Maximum Retry Percent	Percentage of the maximum retries that are allowed. The default value is 80. If it exceeds 80, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

Table 5-139   Media Stream Multicast Direct Parameters

Parameters	Description
Multicast Direct Enable	Multicast direct for this radio. This parameter is enabled by default.
Max Streams per Radio	Maximum number of streams allowed per radio. The range is 0 to 20. The default value is set to auto. If you choose auto, then there is no limit set for the number of client subscriptions.
Max Streams per Client	Maximum number of streams allowed per client. The range is 0 to 20. The default value is set to auto. If you choose auto, then there is no limit set for the number of client subscription.
Best Effort QoS Admission	If enabled, the controller admits the media stream in the best radio queue for this radio. The default is disabled.

802.11b/g EDCA Parameters

Choose **WIRELESS > 802.11b/g/n > EDCA Parameters** to navigate to the EDCA Parameters page.

This page enables you to configure enhanced distributed channel access (EDCA) parameters. EDCA parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.

> **Note**   You must disable the radio network before configuring EDCA parameters. To disable the radio network, go to the 802.11b/g/n Global Parameters page, unselect the **802.11b/g Network Status** check box, and click **Apply**.
>
> After you configure the EDCA parameter, reenable the radio network. To reenable the radio network, go to the 802.11b/g/n Global Parameters page, check the **802.11b/g Network Status** check box, and click **Apply**.

This table describes the EDCA general parameters.

Table 5-140   EDCA General Parameters

Parameter	Description
EDCA Profile	Choose one of the following options from the EDCA Profile drop-down list: • WMM—(Default) Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network. • Spectralink Voice Priority—Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls. • Voice Optimized—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network. • Voice & Video Optimized—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network. **Note** If you deploy video services, admission control (ACM) must be disabled from the 802.11b/g/n Video Parameters page.
Enable Low Latency MAC	MAC optimization for voice that you can enable or disable. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, thereby improving the number of voice calls serviced per access point.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11n (2.4 GHz) High Throughput

Choose **WIRELESS > 802.11b/g/n > High Throughput (802.11n)** to navigate to the High Throughput page.

This page enables you to configure 802.11n support on the network and support of the different Modulation Coding Schemes (MCS) settings. The MCS index determines the number of spatial streams, the modulation, the coding rate, and data rate values.

This table describes the 802.11n (2.4 GHz) high throughput parameters.

Table 5-141   802.11n (2.4 GHz) High Throughput Parameters

Parameter	Description
11n Mode	802.11n mode on the network that you can enable or disable. The default is enabled.
MCS (Data Rate) Settings (0 through 23)	Support for a specific MCS that you can enable or disable. By default all MCS data rate settings are enabled.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

802.11b CleanAir

To configure Cisco CleanAir functionality on the 802.11b/g/n network using the controller GUI, follow these steps:

Step 1   Choose **Wireless > 802.11b/g/n > CleanAir** to navigate to the 802.11b/g/n CleanAir page.

> **Note**   Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

Step 2   Select the **CleanAir** check box to enable CleanAir functionality on the 802.11b/g/n network, or unselect it to prevent the controller from detecting spectrum interference. The default is enabled.

Step 3   Select the **Report Interferers** check box to enable the CleanAir system to report any detected sources of interference, or unselect it to prevent the controller from reporting interferers. The default is enabled.

> **Note**   Device Security alarms, Event Driven RRM, and Persistence Device Avoidance algorithm will not work if Report Interferers is disabled.

Step 4   Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points associated with the same controller. Persistent interferers are present at the location and interfere with the WLAN operations even if they are not detectable at all times

Step 5   Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect multiple select text box and any that do not need to be detected appear in the Interferences to Ignore multiple select text box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interference sources are detected. The possible sources of interference include the following:

- Canopy—A canopy bridge device
- Continuous Transmitter—A continuous transmitter
- DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone

- Jammer—A jamming device

- SuperAG—An 802.11 SuperAG device

- TDD Transmitter—A time division duplex (TDD) transmitter

- Video Camera—A video camera

- WiFi Invalid Channel—A device using nonstandard Wi-Fi channels

- WiFi Inverted Channel—A device using spectrally inverted Wi-Fi signals

- WiMAX Fixed—A WiMAX fixed device (802.11a/n/ac only)

- WiMAX Mobile—A WiMAX mobile device (802.11a/n/ac only)

Note   Access points associated to the controller send interference reports only for the type of interferer devices that appear in the Interferences to Detect text box. This functionality enables you to filter out source of interference that you do not want as well as any that may be flooding the network and causing performance problems for the controller or Cisco PI. Filtering allows the system to resume normal performance levels.

Step 6   Configure CleanAir alarms as follows:

   a.   Select the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or unselect the check box to disable this feature. The default value is selected.

   b.   If you selected the Enable AQI Trap check box in the step above, enter a value between 1 and 100 (inclusive) in the AQI Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default is 35.

- Enter the **AQI Alarm Threshold (1 to 100)** that you want to set. An alarm is generated when the air quality reaches a threshold value. The default is 35. The valid range is between 1 and 100.

- Select the **Enable trap for Unclassified Interferences** check box to enable the traps to be generated for unclassified interferences. Cisco CleanAir can detect and monitor unclassified interferences. Unclassified interferences are interferences that are detected but do not correspond to any of the known interference types.

- Enter the **Threshold for Unclassified category trap (1 to 99)**. Enter a value between 1 and 99. The default is 20. This configuration enables traps to be sent at a set threshold.

   c.   Select the **Enable Interference For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect the check box to disable this feature. The default value is selected.

   d.   Make sure that any sources of interference that need to trigger interferer alarms appear in the Trap on These Types multiple select text box and any that do not need to trigger interferer alarms appear in the Do Not Trap on These Types text box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.

For example, if you want the controller to send an alarm when it detects a jamming device, select the **Enable Interference Type Trap check box** and move the jamming device to the Trap on These Types multiple select box.

Step 7   The Event Driven RRM section displays the current status or the event-driven radio resource management configured on this radio:

- EDRRM—Displays the current status of the spectrum event-driven RRM.

- Sensitivity Threshold—Displays the threshold level at which the event-driven RRM is invoked.

✎

Note   If you want to change the current status of event-driven RRM or the sensitivity level, click **Change Settings**. The **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page appears.

Step 8   Click **Apply** to commit your changes.

Configuring Media Stream

Choose **WIRELESS > Media Stream > General** to navigate to the Media Stream > General page.

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. As a result, lost or corrupted packets are not sent and may cause an IP multicast stream to be not viewable.

This page allows you to enable or disable multicast direct support on the network. Additionally, you can also configure an acknowledgement mechanism in which an acknowledgment is sent to clients when the access point receives multicast frames.

This table describes the media stream general parameters.

Table 5-142   Media Stream General Parameters

Parameter	Description
Multicast Direct Feature	Multicast direct that you can enable or disable. The default is enabled.
	Note Enabling the Multicast feature does not automatically reset the existing client state. You must reset the multicast direct-enabled WLAN and 802.11 networks to clear clients.
Session Message Config	
Session announcement State	Session announcement mechanism to the client. If enabled, clients are informed every time the controller is not able to serve multicast-direct data to the client. The default is unselected.
Session announcement URL	URL where the client can find more information when errors occur during multicast media stream transmission.
Session announcement Email	E-mail ID of the person who can be contacted.
Session announcement Phone	Phone number of the person who can be contacted.
Session announcement Note	Reason as to why a particular client cannot be served with a multicast media.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Media Streams

Choose **WIRELESS > Media Stream > Streams** to navigate to the Media Streams page.

This page enables you to list all the multicast media streams configured on the controller.

This table describes the media stream parameters.

Table 5-143   Media Stream Parameters

Parameter	Description
Stream Name	Multicast media stream name.
Start IP Address	Starting IP address (IPv4 or IPv6) of the media stream for which the multicast direct feature is enabled.
End IP Address	Ending IP address (IPv4 or IPv6) of the media stream for which the multicast direct feature is enabled.
Operational Status	Operational status of this media stream.

Click **Add New** to configure a new media stream. See the "Configuring a New Media Stream and Enabling the Media Stream" topic.

Click **Delete All** delete the multicast media streams.

Configuring a New Media Stream and Enabling the Media Stream

To configure a new media stream, follow these steps:

Step 1   Choose **WIRELESS > Media Stream > Streams** to navugate to the Media Streams page.

Step 2   Click **Add New** to configure a new media stream.

Step 3   Specify the following details for the new stream as follows:

Note   The Stream Name, Multicast Destination Start IP Address, and Multicast Destination End IP Address text boxes are mandatory. You must enter information in these text boxes.

- Stream Name—Specifies a unique name to the stream. The stream name can be up to 64 characters.
- Multicast Destination Start IP Address—Specifies the starting IP address (IPv4 or IPv6) of the multicast media stream.
- Multicast Destination End IP Address—Specifies the ending IP address (IPv4 or IPv6) of the multicast media stream.
- Maximum Expected Bandwidth (1 to 35000 Kbps)—Specifies the maximum expected bandwidth that you want to assign to the media stream. The values can range between 1 to 35000 Kbps.

Note   We recommend that you use a template to add a media stream to the controller.

Step 4   From the Select from Predefined Templates drop-down list under Resource Reservation Control (RRC) Parameters, choose one of the following options to specify details about the resource reservation control:

- Very Coarse (below 300 Kbps)

- Coarse (below 500 Kbps)

- Ordinary (below 750 Kbps)

- Low (below 1 Mbps)

- Medium (below 3 Mbps)

- High (below 5 Mbps)

> **Note**   When you select a template from the drop-down list, the following text boxes under the Resource Reservation Control (RRC) Parameters list their default values that are assigned with the template.

- Average Packet Size (100–1500 bytes)—Specifies the average packet size. The range is 100 to 1500 bytes. The default value is 1200.

- RRC Periodic update—Enables the RRC Periodic update. The RRC Decision message is periodically sent to the access point to update the media stream status. This message is sent at the time of admission and re-RRC calculations. The default is enabled.

- RRC Priority (1–8)—Specifies the priority bit set in the media stream. The priority can be any number from 1 to 8. The larger the value means the higher the priority is. For example, a priority of 1 is the lowest value and a value of 8 is the highest value. The default priority is 4. The low priority stream may be denied in the RRC periodic update.

- Traffic Profile Violation—Specifies the action to perform in case of a violation after a re-RRC. Select an action from the drop-down list. The possible values are as follows:

    – Drop—Specifies that a stream is dropped on periodic revalation.

    – Fallback—Specifies that a stream is demoted to best-effort class on periodic reevaluations.

    The default is **Drop**.

Step 5   Click **Apply** to save the configuration changes.

> **Note**   To enable the media stream using the controller GUI, perform Step 5 to Step 8.

> **Note**   The media stream added needs to be enabled for multicast-direct.

Step 6   Choose **WLANs > WLAN ID** to open the WLANs > Edit page.

Step 7   Choose the **QoS** tab and select **Gold** (Video) from the Quality of Service (QoS) drop-down list.

Step 8   Enable **Multicast Direct**.

Step 9   Click **Apply** to save the configuration changes.

Application Visibility and Control

Application Visibility and Control (AVC) uses the Network Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1500 Layer 4 to Layer 7 protocols. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades. AVC recognizes applications and passes this information to other features like QoS, NetFlow, or firewall, which can take action based on the classification

Guidelines

- Only WLANS on local mode access points, or centrally switched on FlexConnect access points can have applications recognized by NBAR.

- Only IPv4 traffic can be analyzed using AVC.

Note   AVC is supported only on the Cisco 2500 and 5500 Series Wireless Controllers, Cisco WiSM2, and Cisco Flex 7500 Series Wireless Controllers and Cisco 8500 Series Wireless Controllers,

Choose **WIRELESS > Application Visibility and Control** to navigate to this page. From here, you can choose the following:

- **WIRELESS > Application Visibility and Control > Applications** to view all the supported applications.

  See AVC Applications for more information.

- **WIRELESS > Application Visibility and Control > Profiles** to add new and view existing profiles to the controller.

  See AVC Profiles for more information.

AVC Applications

Choose **WIRELESS > Application Visibility and Control > Applications** to navigate to the AVC Applications page. This page enables you to view details of all the 1536 applications.

This table describes the AVC application parameters.

Parameter	Description
Application Name	Name of the application.
Application Group	Name of the application group to which the application belongs. The supported application groups are as follows: • Browsing • Business and productivity tools • Email • File sharing • Gaming • Industrial protocols • Instant messaging • Internet privacy • Layer3 over IP • Location-based services • Net admin • Newsgroup • Obsolete • Other • Trojan • Voice and video
Application ID	Unique ID assigned to the application.
Engine ID	Engine ID assigned to each application by the NBAR engine. This ID is used by Prime Assurance Manager (PAM) to display application names.
Selector ID	Selector ID assigned to each application by the NBAR engine. This ID is used by PAM to display application names.

To view all classified applications, choose **Monitor > Applications**, click the WLAN ID to navigate to the Monitor > Clients page.

AVC Profiles

Choose **WIRELESS > Application Visibility and Control > Profiles** to navigate to the AVC Profiles page.

This page allows you to view the AVC profiles configured on the Cisco WLC.

Guidelines

- You can configure only one AVC profile per WLAN.

- Each AVC profile can have up to 32 rules.

- Each rule states a Mark or Drop action for an application, which allows you to configure up to 32 application actions per WLAN.

- You can configure up to 16 AVC profiles on a controller.

- You can associate an AVC profile with multiple WLANs.

- AVC profiles do not support AAA Override.

- AVC profiles are applied per WLAN and not per user.

To delete an AVC profile, click the blue arrow adjacent the profile and choose **Remove**.

To add a new AVC profile, click **New**.

Configuring a New AVC Profile and Adding Rules to the Profile

To configure a new AVC profile, follow these steps:

Step 1   Choose **WIRELESS > Application Visibility and Control > Profiles** and click **New** to configure a new AVC profile.

Step 2   Specify the AVC profile name. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Step 3   Click **Apply**. The new AVC profile appears in the list of AVC profiles configured on the Cisco WLC.

Step 4   Click the AVC Profile name to navigate to the AVC Profile > Edit page.

Step 5   Click **Add New Rule** to configure a policy for an application.

Step 6   Specify the following details for the AVC Profile as follows:

Parameter	Description
Application Group	Drop-down list from which you can choose an application group.
Application Name	Drop-down list from which you can choose an application from the chosen application group.

Parameter	Description
Action	Drop-down list from which you can choose the following: • **Drop**—Drops the upstream and downstream packets that correspond to the chosen application. • **Mark**— Marks the upstream and downstream packets that correspond to the chosen application with the DSCP value that you specify in the Differentiated Services Code Point (DSCP) drop-down list. The DSCP value helps you to provide differentiated services based on the QoS levels. If an AVC profile mapped to a WLAN has a rule for MARK action, that application gets precedence according to the QoS profile configured in the AVC rule overriding the QoS profile configured on WLAN. The default action is to permit all applications. NBAR helps identify both high and low priority traffic so that appropriate QoS policy is applied on per WLAN.
DSCP	Packet header code that is used to define QoS across the Internet. The DSCP values are mapped to the following QoS levels: • Platinum (Voice)—Assures a high QoS for Voice over Wireless. • Gold (Video)—Supports the high-quality video applications. • Silver (Best Effort)—Supports the normal bandwidth for clients. • Bronze (Background)— Provides the lowest bandwidth for guest services. You can also choose **Custom** and specify the DSCP value. The range is from 0 to 63.

To edit a rule, click **Add New Rule**, select the application and configure a different action.

Step 7   Click **Apply**.

To apply an AVC profile to all clients in a WLAN, choose **WLANs** and click the Profile name to navigate to the **WLANs > Edit** page.

Lync Server

Microsoft Lync server manages services such as voice, video, application sharing and file transfer for clients. Microsoft has an SDN (software-defined network) support, which if subscribed to, sends information with respect to those calls.

The WLC solution subscribes to the Lync messages and apply relevant QoS Policies to active Lync calls for wireless clients, which belong to a given WLC.

For a detailed implementation information, see http://www.cisco.com/c/dam/en/us/products/collateral/wireless/lync.pdf.

Choose **WIRELESS > Lync Server** to navigate to the **Global Lync Server Configuration** page.

Parameter	Description
Lync Server	Check box to enable global Lync SDN.
Port	Text box to specify the port number that the Lync service has to listen to. This number is arbitrary and is not a fixed port. Ensure that the same number is configured on the Lync Server side as well.
Protocol	Two options: • HTTP • HTTPS We recommend that you use HTTPS.

Country

Choose **WIRELESS > Country** to navigate to the Country page.

On this page, select the country code or codes where the Cisco WLC and associated access points are installed and operational. This selection ensures that the listed broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

For more information on configuring country codes, see the Configuring the Country Code topic.

Note   Generally, you configure one country code per controller, (the one matching the physical location of the controller and its access points). However, you can configure up to 20 country codes per controller. This multiple-country support enables you to manage access points in various countries from a single controller.

For more information on configuring multiple country codes, see the Multiple Country Codes topic.

Note   Both 802.11a/n/ac and 802.11b/g/n networks must be disabled in order to change the country code.

For a complete list of country codes supported per product, refer to this URL:

The currently supported countries are as follows:

http://www.cisco.com/c/en/us/products/collateral/wireless/access-points/product_data_sheet0900aecd8
0537b6a.html

- AE (United Arab Emirates)

- AR (Argentina)

- AT (Austria), which allows 802.11a/n/ac and 802.11b/g/n

- AU (Australia), which allows 802.11a and 802.11b

- BE (Belgium), which allows 802.11a and 802.11b/g

- BH (Bahrain)

- BG (Bulgaria)

- BR (Brazil), which allows 802.11a and 802.11b/g

- CA (Canada), which allows 802.11b/g

- CA2 (Canada) DCA excludes UNII-2

- CH (Switzerland and Liechtenstein), which allows 802.11a and 802.11b/g

- CL (Chile)

- CN (China)

- CO (Colombia)

- CY (Cyprus), which allows 802.11a and 802.11b/g

- CZ (Czech Republic), which allows 802.11a and 802.11b

- DE (Germany), which allows 802.11a and 802.11b/g

- DK (Denmark), which allows 802.11a and 802.11b/g

- DO (Dominican Republic)

- EE (Estonia), which allows 802.11a and 802.11b/g

- ES (Spain), which allows 802.11a and 802.11b/g

- FI (Finland), which allows 802.11a and 802.11b/g

- FR (France), which allows 802.11a and 802.11b/g

- GB (United Kingdom), which allows 802.11a and 802.11b/g

- GI (Gibraltar)

- GR (Greece), which allows 802.11b/g

- HK (Hong Kong), which allows 802.11a and 802.11b/g

- HU (Hungary), which allows 802.11a and 802.11b/g

- ID (Indonesia)

- IE (Ireland), which allows 802.11a and 802.11b/g

- IL (Israel), which allows 802.11a and 802.11b/g

- ILO (Israel Outdoors), which allows 802.11a and 802.11b/g

- IN (India), which allows 802.11a and 802.11b

- IQ (Iraq)

- IS (Iceland), which allows 802.11a and 802.11b/g

- IT (Italy), which allows 802.11a and 802.11b/g

- JP (Japan), which allows 802.11a and 802.11b/g

- J2 (Japan 2 P)

- J3 (Japan 3 U)

- KE (Korea Extended K)

- KR (Republic of Korea), which allows 802.11a and 802.11b/g

- KW (Kuwait)

- LI (Liechtenstein)

- LT (Lithuania), which allows 802.11a and 802.11b/g

- LU (Luxembourg), which allows 802.11a and 802.11b/g

- LV (Latvia), which allows 802.11b/g

- MC (Monaco)

- ME (Montenegro)

- MK (Macedonia)

- MT (Malta)

- MX (Mexico)

- MY (Malaysia), which allows 802.11b/g

- NL (Netherlands), which allows 802.11a and 802.11b/g

- NO (Norway), which allows 802.11a and 802.11b/g

- NZ (New Zealand), which allows 802.11a and 802.11b/g

- OM (Oman)

- PA (Panama)

- PE (Peru)

- PH (Philippines), which allows 802.11a and 802.11b

- PH2 (Philippines (DCA excludes UNII))

- PK (Pakistan)

- PL (Poland), which allows 802.11a and 802.11b/g

- PR (Puerto Rico)

- PT (Portugal), which allows 802.11a and 802.11b/g

- PY (Paraguay)

- QA (Qatar)

- RS (Serbia)

- RU (Russian Federation)

- RO (Romania)

- SA (Saudi Arabia)

- SE (Sweden), which allows 802.11a and 802.11b/g

- SG (Singapore), which allows 802.11a and 802.11b/g

- SI (Slovenia), which allows 802.11a and 802.11b/g

- SK (Slovak Republic), which allows 802.11a and 802.11b/g

- TH (Thailand), which allows 802.11b/g
- TN (Tunisia)
- TR (Turkey)
- TW (Taiwan), which allows 802.11a and 802.11b/g
- UA (Ukraine)
- US (United States of America), which allows an 802.11b/g operation, and 802.11a Low, Medium, and High bands
- USE (USA), which allows 802.11a and 802.11b/g
- USL (USA Low), which allows an 802.11b/g operation, and 802.11a Low and Medium bands. (Used for legacy 802.11a interface cards that do not support 802.11a High band)
- USX (USA Extended), which allows 802.11a and 802.11b/g
- VE (Venezuela)
- ZA (South Africa), which allows 802.11a and 802.11b/g

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Configuring the Country Code

Note   Disable both the 802.11a/n/ac and 802.11b/g/n networks to change the country code.

To configure the country code using the GUI, follow these steps:

Step 1   Disable the 802.11a/n/ac and 802.11b/g/n networks as follows:

    a. Click **Wireless > 802.11a/n/ac > Network**.

    b. Unselect the **802.11a Network Status Enabled** check box.

    c. Click **Apply** to commit your changes.

    d. Click **Wireless > 802.11b/g/n > Network**.

    e. Unselect the **802.11b/g Network Status Enabled** check box.

    f. Click **Apply** to commit your changes.

Step 2   Click **Wireless > Country** to access the Country page.

Step 3   Select the check box for the country where your access point is installed.

Step 4   Click **Apply** to commit your changes.

Step 5   Reenable the 802.11a/n/ac and 802.11b/g/n networks that you disabled in Step 1.

Step 6   Click **Save Configuration** to save your settings.

Multiple Country Codes

You can configure up to 20 country codes for each controller. This multiple-country support enables you to manage access points in various countries from a single controller.

Guidelines

Follow these guidelines when configuring multiple country codes:

- The multiple-country feature is not supported for use with Cisco Aironet 1500 series mesh access points.

- When multiple countries are configured and the radio resource management (RRM) auto-RF feature is enabled, the auto-RF feature is limited to only the channels that are legal in all configured countries and to the lowest power level common to all configured countries. The access points are always able to use all legal frequencies but uncommon channels can only be assigned manually.

- The access point can only operate on the channels for the countries that they are designed for.

> **Note** If an access point is set to a higher legal power level or is configured manually, the power level is limited only by the particular country to which that access point is assigned.

- When multiple countries are configured, the 802.11a/n/ac network is disabled for all the countries if any country does not support the 802.11a radio, or there are no common channels on the 802.11a radio.

- The country list configured on the RF group leader determines what channels the members would operate on. This is independent of what countries have been configured on the RF Group members.

Configuring Multiple Country Codes

> **Note** Disable both the 802.11a/n/ac and 802.11b/g/n networks to change the country code.

To configure country codes using the GUI, follow these steps:

Step 1 Disable the 802.11a/n/ac and 802.11b/g/n networks as follows:

   a. Click **Wireless > 802.11a/n/ac > Network**.

   b. Unselect the **802.11a Network Status Enabled** check box.

   c. Click **Apply** to commit your changes.

   d. Click **Wireless > 802.11b/g/n > Network**.

   e. Unselect the **802.11b/g Network Status Enabled** check box.

   f. Click **Apply** to commit your changes.

Step 2 Choose **Wireless > Country** to access the Country page.

Step 3 Choose the check box for each country where your access points are installed.

Step 4 If you selected more than one check box in Step 3, a message appears indicating that RRM channels and power levels are limited to common channels and power levels. Click **OK** to continue or **Cancel** to cancel the operation.

Step 5   Click **Apply** to commit your changes.

Step 6   Re-enable the 802.11a/n/ac and 802.11b/g/n networks if you did not re-enable them in Step 1.

Step 7   Click **Save Configuration** to save your settings.

Changing Default Country Codes

To see the default country chosen for each access point and to choose a different country if necessary, follow these steps:

✎
Note   If you remove a country code from the configuration, any access points that are assigned to the deleted country are reassigned to one of the remaining countries if possible.

Step 1   Click **Wireless** > **Access Points** > **All APs** to access the All APs page.

Step 2   Click the link for the desired access point.

The default country for the access point appears in the Country Code drop-down list. The drop-down list contains only those country codes that are compatible with the regulatory domain of at least one of the access point's radios.

Step 3   If the access point is installed in a country other than the one shown, choose the correct country from the drop-down list.

Step 4   Click **Apply** to commit your changes.

Step 5   Repeat Step 2 through Step 4 to assign all the access points that are joined to the controller of a specific country.

Step 6   Re-enable the 802.11a/n/ac and 802.11b/g/n networks.

Step 7   Click **Save Configuration** to save your settings.

Timers

Choose **WIRELESS > Timers** to navigate to the Timers page. This page enables you to view the timeout parameter.

This table describes the timer parameters.

Table 5-144   Timer Parameters

Timer	Description
802.11 Authentication Response Timeout	802.11 authentication response timeout that is between 5 and 60 seconds. The default is 10 seconds.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

NetFlow

Choose **WIRELESS > Netflow** to navigate to the Netflow page.

NetFlow is a protocol that provides valuable information about network users and applications, peak usage times, and traffic routing. This protocol collects IP traffic information from network devices to monitor traffic. The NetFlow architecture consists of the following components:

- Collector—An entity that collects all the IP traffic information from various network elements. NBAR exports traffic data to a NetFlow Collector.

- Exporter—A network entity that exports the template with the IP traffic information. The controller acts as an exporter. Configuring an exporter on the controller enables the collection of application statistics for export to an external monitor.

In the controller you can choose the following:

- **WIRELESS > Netflow > Monitor** to configure or view details of the NetFlow monitor and records.

  See Netflow Monitor for more information.

- **WIRELESS > Netflow > Exporter** to view details of the NetFlow exporters.

  See Netflow Exporter for more information.

Netflow Monitor

Choose **WIRELESS > Netflow > Monitor** to navigate to the Monitor page. NetFlow record monitoring and export are used for integration with Cisco Prime Infrastructure or any NetFlow analysis tool.

This table describes the NetFlow monitor parameters.

Table 5-145   NetFlow Monitor Parameters

Parameter	Description
Monitor Name	Name of the NetFlow monitor. The monitor name can be up to 127 case-sensitive, alphanumeric characters. You cannot include spaces within a monitor name. You can configure only one monitor in the controller.
Record Name	Name of the NetFlow record. A NetFlow record in the controller contains the following information about the traffic in a given flow: • Client MAC address • Client source IP address • WLAN ID • Application ID • Incoming bytes of data • Outgoing bytes of data • Incoming packets • Outgoing packets • Incoming DSCP • Outgoing DSCP • Name of the last AP
Exporter Name	Name of the exporter. You cannot include spaces within an exporter name. You can configure only one monitor in the controller.
Exporter IP	IP address of the collector.
Port	UDP port through which the NetFlow record is exported from the controller.

Click **New** to add a new NetFlow monitor.

Netflow Exporter

Choose **WIRELESS > Netflow > Exporter** to navigate to the Exporter page.

This table describes the NetFlow exporter parameters.

Table 5-146   NetFlow Exporter Parameters

Parameter	Description
Exporter Name	Name of the exporter. You can configure only one exporter on the controller. You cannot include spaces within an exporter name.
Exporter IP	IP address of the exporter.
Port Number	UDP port through which the NetFlow record is exported.

QoS Profiles

Choose **WIRELESS > QoS > Profiles** to navigate to the QoS Profiles page. This page enables you to view the quality of service (QoS) settings.

This table describes the QoS profiles parameters.

Table 5-147   QoS Profiles

Parameter	Description
Profile Name	Name of the QoS profile.
Description	Platinum (Voice)—Assures a high quality of service for Voice over Wireless. Gold (Video)—Supports high-quality video applications. Silver (Best Effort)—Supports the normal bandwidth for clients. This setting is the default. Bronze (Background)—Provides the lowest bandwidth for guest services. VoIP clients should be set to Platinum while low-bandwidth data clients can be set to Silver or Bronze.

Click the profile name to go to the Editing QoS Profile page and specify how much bandwidth a client is allocated in the network for that QoS profile.

Editing QoS Profile

Choose **WIRELESS > QoS > Profiles** and then click the profile name to navigate to the Edit QoS Profile page.

The top of the main page lists the selected quality of service (QoS) profile name.

This table describes the QoS profile parameters.

Table 5-148   QoS Profile Parameters

Parameter	Description
QoS Profile Name	Name of the QoS profile.
Description	User-defined description for this QoS profile.
Per-User Bandwidth and Per-SSID Bandwidth Contracts	
Note	When you set the Per-User Bandwidth Contracts parameters to 0 (OFF), the traffic allowed is unlimited and is restricted by only other 802.11 limitations.
Average Data Rate	User-defined average data rate (kbps) for non-UDP traffic. Valid values are from 0 to 60,000; the default is 0 (OFF).
Burst Data Rate	User-defined peak data rate (kbps) for non-UDP traffic. Valid values are from 0 to 60,000; the default is 0 (OFF).
Average Real-Time Rate	User-defined average data rate (kbps) for UDP traffic. Valid values are from 0 to 60,000; the default is 0 (OFF).

Table 5-148   QoS Profile Parameters

Parameter	Description
Burst Real-Time Rate	User-defined peak data rate (kbps) for UDP traffic.
	Valid values are from 0 to 60,000; the default is 0 (OFF).
WLAN QoS Parameters	
Maximum Priority	Maximum QoS priority for the WLAN of the profile.
	Available options are as follows:
	• besteffort
	• background
	• video
	• voice
Unicast Default Priority	Default QoS priority of unicast packet for the WLAN of the profile.
	Available options are as follows:
	• besteffort
	• background
	• video
	• voice
Multicast Default Priority	Default QoS priority of multicast packet for the WLAN of the profile.
	Available options are as follows:
	• besteffort
	• background
	• video
	• voice
Wired QoS Protocol	
Protocol Type	Protocol type. Choose **802.1P** to activate 802.1P Priority Tags, or choose **None** to deactivate 802.1P Priority Tags (default).
802.1P Tag	802.1P priority tag for the wired connection that is used for traffic and CAPWAP packets. Valid values are from 0 to 7.
	The default values are 1 for Bronze, 3 for Silver, 4 for Gold, and 6 for Platinum.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Click **Reset to defaults** to reset the parameters to the factory default.

QoS Roles for Guest Users

Choose **WIRELESS > QoS > Roles** to navigate to the QoS Roles for Guest Users page.

This page enables you to view the quality of service (QoS) roles for guest users.

Choose **New** to display the Creating New QoS Roles page and to create a new QoS role.

Click the role name to display the Editing QoS Role Data Rates page and specify how much bandwidth a wired guest user is allocated in the network for that QoS role.

> **Note**   After you create the QoS role for guest user, you can assign a role to a guest user from the Local Net Users page.

To delete a role, click the blue arrow adjacent the desired access point and choose **Remove**.

To add a new role, click **New**.

Creating New QoS Roles

Choose **WIRELESS > QoS > Roles** and then click **New** to navigate to the QoS Role Name > New page.

This page enables you to create quality of service roles for guest users. Click the profile name to go to the Editing QoS Role Data Rates page and edit the QoS role parameters.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing QoS Role Data Rates

Choose **WIRELESS > QoS > Roles**, and then click the role name to navigate to the Edit QoS Role data rates page.

This page enables you to specify bandwidth limits for guest users of different roles. The top of the main page lists the selected role name.

This table describes the QoS role parameters.

Table 5-149   QoS Role Parameters

Parameter	Description
Note	When you set the Per-User Bandwidth Contracts parameters to 0 (OFF), the traffic allowed is unlimited and is restricted only by other 802.11 limitations.
Average Data Rate	Operator-defined average data rate (kbps) for non-UDP traffic.
	Valid values are from 0 to 60,000; the default value is 0 (OFF).
Burst Data Rate	Operator-defined peak data rate (kbps) for non-UDP traffic.
	Valid values are from 0 to 60,000; the default value is 0 (OFF).
Average Real-Time Rate	Operator-defined average data rate (kbps) for UDP traffic.
	Valid values are from 0 to 60,000; the default value is 0 (OFF).
Burst Real-Time Rate	Operator-defined peak data rate (kbps) for UDP traffic.
	Valid values are from 0 to 60,000; the default value is 0 (OFF).

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.