Managing APs

Access Point Modes

Each lightweight AP is configured to operate in one of several different AP modes. In some modes, the AP provides network service to clients; in other modes, the AP operates as a dedicated network management tool.

Not all AP models support all AP modes.

Client-Serving AP Modes

- **Local**: This is the default mode. A local mode AP tunnels all client traffic, for all WLANs, in CAPWAP, to the controller. In this mode, the AP's radios are operational only when the AP is connected to its controller. Local mode APs do not support mesh operation. All AP models support Local mode.
- **FlexConnect**: In this mode, client traffic can either be tunneled in CAPWAP to the controller, or egress at the AP's LAN port, depending on the WLAN configuration. FlexConnect mode APs do not support mesh operation. All models support FlexConnect mode.
- **Bridge and Flex+Bridge**: These modes are used in mesh deployments, where wireless rather than wired backhaul is used for CAPWAP connectivity. Not all AP models support these modes; see the relevant mesh documentation for information about support for mesh operation.

Network Management AP Modes

- **Monitor**: In this mode, the AP radios are dedicated to monitoring the Wi-Fi channel for RRM and rogue detection. All AP models support this mode.
- **Rogue Detector**: In this mode, the AP radios are disabled; the AP monitors the LAN to detect on-wire rogue activity. This mode is not supported on Cisco Wave 2 or 802.11ax APs and is deprecated.
- **Sniffer**: In this mode, the AP radio operates in promiscuous mode and captures all Wi-Fi traffic on a channel. These packets are tunneled in CAPWAP to the controller, which forwards them to a machine running OmniPeek or Wireshark for storage and analysis.
- **SE-Connect**: In this mode, the AP provides a dedicated connection to CleanAir for spectrum analysis by software such as Spectrum Expert or Chanalyzer. SE-Connect mode is supported only on SE models with CleanAir.

Global Credentials for Access Points

Cisco IOS access points are shipped from the factory with *Cisco* as the default enable password. This password allows users to log on to the nonprivileged mode and enter **show** and **debug** commands, which poses a security threat. The default enable password must be changed to prevent unauthorized users from accessing to the access point's console port and entering configurable commands.

The following are some guidelines to configure global credentials for access points:

- You can set a global username, password, and enable password that all access points that are currently joined to the controller and any that join in the future inherit as they join the controller. If desired, you can override the global credentials and assign a unique username, password, and enable password for a specific access point.
- After an access point joins the controller, the access point enables console port security, and you are prompted for your username and password whenever you log in to the access point’s console port. When you log on, you are in nonprivileged mode, and you must enter the enable password in order to use the privileged mode.
- The global credentials that you configure on the controller are retained across controller and access point reboots. They are overwritten only if the access point joins a new controller that is configured with a global username and password. If the new controller is not configured with global credentials, the access point retains the global username and password configured for the first controller.
- You must keep track of the credentials used by the access points. Otherwise, you might not be able to log onto the console port of the access point. 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 factory-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, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Clear All Config** on the controller GUI, or enter the **clear ap config** *Cisco_AP* command on the controller CLI. To clear the access point's configuration except its static IP address, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Clear Config Except Static IP**, or enter the **clear ap config** *ap-name* **keep-ip-config** command on the controller CLI. After the access point rejoins a controller, it adopts the default *Cisco*/*Cisco* username and password.

Note If the AP is in Bridge mode, then the same Bridge mode is retained after the factory reset of the AP; if the AP is in FlexConnect, Local, Sniffer, or any other mode, then the AP mode is set to Local mode after the factory reset of the AP. If you press the Reset button on the AP and perform a true factory reset, then the AP moves to a cookie configured mode.

Note Suppose you configure an indoor Cisco AP to go into the mesh mode. If you want to reset the Cisco AP to the local mode, use the **test mesh mode local** command.

- To reset the AP hardware, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Reset AP Now**.

This section contains the following subsections:

Restrictions for Global Credentials for Access Points

- The controller software features are supported on all access points that have been converted to lightweight mode except the 1100 series. VxWorks access points are not supported.
- Telnet is not supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs.
- A global Access Point login credentials once configured in controller cannot be removed.

Configuring Global Credentials for Access Points

Configuring Global Credentials for Access Points (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

Step 2 In the **Username** field, enter the username that is to be inherited by all access points that join the controller.

Step 3 In the **Password** field, enter the password that is to be inherited by all access points that join the controller.

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.
- The AP passwords or secret passwords should not contain the following characters:

  &, <, >, ", and '

Step 4 In the Enable Password text box, enter the enable password that is to be inherited by all access points that join the controller.

Step 5 Click **Apply** to send the global username, password, and enable password to all access points that are currently joined to the controller or that join the controller in the future.

Step 6 Click **Save Configuration** to save your changes.

Step 7 (Optional) Override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point as follows:

a) Choose **Access Points** > **All APs** to open the All APs page.
b) Click the name of the access point for which you want to override the global credentials.
c) Choose the **Credentials** tab. The All APs > Details for (Credentials) page appears.
d) Select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global username, password, and enable password from the controller. The default value is unselected.
e) In the Username, Password, and Enable Password text boxes, enter the unique username, password, and enable password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

f) Click **Apply** to commit your changes.
g) Click **Save Configuration** to save your changes.

Note If you want to force this access point to use the controller's global credentials, unselect the **Over-ride Global Credentials** check box.

Configuring Global Credentials for Access Points (CLI)

Procedure

Step 1 Configure the global username, password, and enable password for all access points currently joined to the controller as well as any access points that join the controller in the future by entering this command:

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password* **all**

Step 2 (Optional) Override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point by entering this command:

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password Cisco_AP*

The credentials that you enter in this command are retained across controller and access point reboots and if the access point joins a new controller.

Note If you want to force this access point to use the controller's global credentials, enter the **config ap mgmtuser delete** *Cisco_AP* command. The following message appears after you execute this command: "AP reverted to global username configuration."

Step 3 Enter the **save config** command to save your changes.

Step 4 Verify that global credentials are configured for all access points that join the controller by entering this command:

show ap summary

Note If global credentials are not configured, the Global AP User Name text box shows "Not Configured."

To view summary of specific access point you can specify the access point name. You can also use wildcard searches when filtering for access points.

Step 5 See the global credentials configuration for a specific access point by entering this command:

show ap config general *Cisco_AP*

Note The name of the access point is case sensitive.

Note If this access point is configured for global credentials, the AP User Mode text boxes shows "Automatic." If the global credentials have been overwritten for this access point, the AP User Mode text box shows "Customized."

Configuring Telnet and SSH for Access Points

Configuring Telnet and SSH for APs (GUI)

Note Telnet is not supported on Cisco Wave 2 and 802.11ax APs.

After you upgrade to Release 8.10.112.0, the AP-specific SSH setting changes to disabled state. However, the APs that have global SSH settings are not impacted.

If you want to retain AP-specific SSH setting, you must explicitly enable SSH on those APs.

Procedure

Step 1 Global configuration:

a) Choose **Wireless** > **Access Points** > **Global Configuration**.

b) In the **Global Telnet SSH** area, check or uncheck **Telnet** and **SSH** check boxes.

When you enable Telnet or SSH for all APs, the functionality is allowed on APs that are yet to join the controller regardless of their mode.

c) Click **Apply**.
d) Click **Save Configuration**.

Step 2 Configuration for a specific AP:

a) Choose **Wireless** > **Access Points** > **All APs**.
b) Click an AP name.
c) Click the **Advanced** tab.
d) From the **Telnet** drop-down list, choose **AP Specific** and check the check box to enable the functionality for the AP.
e) From the **SSH** drop-down list, choose **AP Specific** and check the check box to enable the functionality.
f) Click **Apply**.
g) Click **Save Configuration**.

Configuring Telnet and SSH for APs (CLI)

Note Telnet is not supported on Cisco Wave 2 and 802.11ax APs.

After you upgrade to Release 8.10.112.0, the AP-specific SSH setting changes to disabled state. However, the APs that have global SSH settings are not impacted.

If you want to retain AP-specific SSH setting, you must explicitly enable SSH on those APs.

Procedure

- Configure Telnet or SSH for all APs or a specific AP by entering this command:

  config ap {**telnet** | **ssH**} {**enable** | **disable**} {*ap-name* | **all**}

- Replace the Telnet or SSH configuration for a specific AP with the global configuration by entering this command:

  config ap {**telnet** | **ssH**} **default** *ap-name*

Cisco Access Point with Tri-Radio

Access Points with three radios are designed for high density environments. The APs by default runs one dedicated 2.4-GHz 4x4 radio and one 5-GHz 8x8 mode radio. In the default mode, the radios are managed by the Flexible Radio Assignment (FRA), and the Dual Radio Mode is in disabled state indicating that the radios have either been assigned as client serving 8x8 radio or have not yet been evaluated by FRA.

If you enable Dual Radio Mode setting, the 8x8 radio is split to two independent 5-GHz 4x4 radios. In this mode, the first 5-GHz radio and second 5-GHz radio are active independent 4x4 radio interfaces. They can serve different user groups with different assigned channels.

Note To disable dual radio mode, you must first disable the admin status of the subordinate radio. Else, you are prompted with a warning message.

A tri-radio AP has upto two configurable 5-GHz radios. The following table illustrates the radio role and its deployment benefits.

Table 1: 5-GHz Radio Operational Modes and Criteria

Radio Role		Driving Factors
Radio 1	**Radio 2**	
8x8 Client-Serving for non-160 MHz clients 4x4 Client-Serving for 160 MHz clients	None	• Operates at 8x8 for 20/40/80 MHz • Higher MU-MIMO stations • Better channel reuse in very high density conditions • Required higher number of Spatial Streams (SS)
4x4 Client-Serving	4x4 Client-Serving	• Preferred operation: 80 MHz or below • High Capacity in low or medium density • Directional antenna units (Coverage Slicing)
4x4 Client-Serving	4x4 Monitor	• Preferred operation: 80 MHz or below • Lower MU-MIMO stations • Better channel reuse in high density • Monitoring application requires 4x4 Rx

The following table lists the different radio modes and roles supported by the AP.

Table 2: Tri-Radio AP Radio Configuration

Setup	Radio Mode	Maximum Radio Capability	Dual Role Mode
1	2.4-GHz + 5-GHz	2.4-GHz, 4 antennas, 4SS, and 20 MHz 5-GHz, 8 antennas, 4SS, and 160 MHz	Disabled

Setup	Radio Mode	Maximum Radio Capability	Dual Role Mode
2	2.4-GHz + 5-GHz	2.4-GHz, 4 antennas, 4SS, and 20 MHz 5-GHz, 8 antennas, 8SS, and 80 MHz	Disabled
3	2.4-GHz + 5-GHz + 5-GHz	2.4-GHz, 4 antennas, 4SS, and 20 MHz 5-GHz, 4 antennas, 4SS, and 80 MHz 5-GHz, 4 antennas, 4SS, and 80 MHz	Enabled

In a tri-radio AP, similar to other Cisco FRA supporting APs, you can either set the role to be chosen automatically or manually select the role as client-serving or monitor role. Based on the dual radio mode configuration, the role selection is available for both or one interface.

Guidelines and Restrictions for Tri-Radio Access Points

- Dual radio mode is disabled in manual mode by default.
- You need to manually enable the slot 2 radio on the AP. Default setting is disabled.
- The AP reboots without notification when the dual radio mode is changed.
- The tri-radio function for AP with external antenna:
  - is supported with Cisco AP and RP-TNC antenna
    - AIR-CAB-002-D8-R=
    - AIR-CAB-003-D8-N=
  - is not supported with Cisco AP and C-ANT9103 antenna

Configuring Tri-Radio Parameters for an AP (GUI)

Procedure

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

Step 2 Hover your cursor over the blue drop-down arrow for the desired AP, and click **Configure**.

The **802.11a/n/ac/ax** or **802.11b/g/n/ax Cisco APs > Configure** page appears.

Step 3 From the **Dual Radio Assignment** > **Dual Radio Mode** drop-down list, with a Tri-radio capable AP, choose **Enable**.

This splits the 8x8 radio to two 4x4 radios.

Step 4 Select the Dual Radio mode.

Select **Auto** to allow FRA to manage radio mode. Select **Manual** to choose the radio mode for the AP.

Step 5 From the **Radio Role Assignment** options, select the preferred role assignment mode:

- Select **Auto** to allow Dynamic Channel Assignment (DCA) to assign the role to the radios.
- Select **Manual** to manually select the **Client Serving** or **Monitor** role for the radio interface.

Step 6 Specify the RF Channel Assignment from the following options:

- **Global**: Choose this to specify a global value
- **Custom**: Choose this and then select the **Channel Width** from the drop-down list to specify a custom value

Step 7 Click **Apply**.

Configuring Dual Radio on a Tri-Radio AP (CLI)

Procedure

- Configure dual radio mode by entering this command:

  config {**802.11a** | **802.11b** } **dualradio** {**global** | **ap** *ap-name*}**manual** {**enable** | **disable** }

Note You need to disable slot-1 radio before enabling dual-radio on the AP.

- Configure dual radio mode for an AP interface by entering this command:

  config slot *slot_id* **dualradio** *ap-name* **manual** {**enable** | **disable** }

Configuring Radio Role on a Tri-Radio AP (CLI)

Procedure

- Configure radio role for a 802.11 network by entering this command:

  config {**802.11a** | **802.11b** } **role** *ap-name* {**auto** | **manual** {**client-serving** | **monitor** } }

- Configure radio role for a radio interface by entering this command:

  config slot *slot_id* **role** *ap-name* {**auto** | **manual** {**client-serving** | **monitor** } }

Spectrum Expert Connection

To obtain detailed spectrum data that can be used to generate RF analysis plots similar to those provided by a spectrum analyzer, you can configure a Cisco CleanAir-enabled access point to connect directly to a Microsoft Windows XP or Vista PC running the Spectrum Expert application (referred to as a *Spectrum Expert console*). You can initiate the Spectrum Expert connection semi-automatically from Prime Infrastructure or by manually launching it from the controller. This section provides instructions for the latter.

Note The Cisco Aironet Access Point Module for Wireless Security and Spectrum Intelligence (WSSI) for the Cisco Aironet 3600 Series Access Point tightly couples data connectivity, spectrum analysis, and security threat detection and mitigation into a single, multipurpose access point. With WSSI you have to use Metageek Chanalyzer Pro with CleanAir support and not Spectrum expert for wIPS, CleanAir and spectrum analysis.

This section contains the following subsections:

Guidelines and Limitations for Spectrum Expert Connection

You may encounter the error message **Unable to contact the remote sensor** while connecting to the Cisco Catalyst 9120 AP. This error message appears due to a difference in the AP architecture compared to the Cisco Wave 2 APs. You can view the 5G data by switching the Spectrum Expert panel to sensord using Slot #0.

Configuring Spectrum Expert (GUI)

Before you begin

Prior to establishing a connection between the Spectrum Expert console and the access point, make sure that IP address routing is properly configured and the network spectrum interface (NSI) ports are open in any intervening firewalls.

Note Starting in Release 8.9, NSI ports can be blocked on APs. Prior to Release 8.9, the NSI ports were always open and it was not possible to block them on APs.

Note Prior to establishing a connection between the Spectrum Expert or Chanalyzer Pro application and the AP, make sure the NSI ports are open on the AP.

Procedure

Step 1 Ensure that Cisco CleanAir functionality is enabled for the access point that will be connected to the Spectrum Expert console.

Step 2 [Optional] Configure the NSI TCP ports (37540 and 37550) on an AP to open or disable them. Or verify the status of these ports before using the Spectrum Expert or Chanalyzer application.

Using the controller GUI, follow these steps:

a) Choose **Wireless** > **Access Points** > **All APs** to open the **All APs** page.
b) Click the name of the desired access point to open the **All APs** > **Details** page.
c) Click the **Advanced** tab.
d) From the **NSI Ports State** drop-down list, choose **AP Specific** and select the check box to enable the functionality for the AP.
e) Click **Apply** to commit your changes.

Using the CLI, follow these steps:

a) To globally configure the NSI ports, enter this command:

config ap nsi-ports { **enable** | **disable** } { **all** | *ap_name* }

b) To configure the NSI ports on a specific AP, enter this command:

config ap nsi-ports default *ap_name*

c) To verify the the status of the NSI ports on the AP, enter this command:

show ap config general *ap_name*

Information similar to the following appears:

```
(device) >show ap config general AP5GC.2331A

Cisco AP Identifier.............................. 3430
Cisco AP Name.................................... AP5GC.2331A
Country code..................................... Multiple Countries : IN,J4,US
Regulatory Domain allowed by Country............. 802.11bg:-AJPQU  802.11a:-ABDJ
                  NPQU
AP Country code.................................. J4 - Japan 4(Q)
AP Regulatory Domain............................. 802.11bg:-Q    802.11a:-Q
Switch Port Number .............................. 3
MAC Address...................................... 5c:a1:78:dw:8a:5a
IP Address Configuration......................... Static IP assigned
IP Address....................................... 192.78.144.23
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 192.78.144.1
Domain.......................................
Name Server.....................................
NAT External IP Address.......................... None
CAPWAP Path MTU.................................. 1485
DHCP Release Override............................ Disabled
Telnet State..................................... Globally Enabled
Ssh State........................................ Globally Enabled
NSI Ports State.................................. Globally Enabled
Virtual IP Address............................... Not Configured
```

Step 3 Configure the access point for SE-Connect mode using the controller GUI or CLI.

Note The SE-Connect mode is set for the entire access point, not just a single radio. However, the Spectrum Expert console connects to a single radio at a time.

If you are using the controller GUI, follow these steps:

a) Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

b) Click the name of the desired access point to open the All APs > Details for page.
c) Choose **SE-Connect** from the AP Mode drop-down list. This mode is available only for access points that are capable of supporting Cisco CleanAir functionality. For the SE-Connect mode to appear as an available option, the access point must have at least one spectrum-capable radio in the Enable state.
d) Click **Apply** to commit your changes.
e) Click **OK** when prompted to reboot the access point.

If you are using the CLI, follow these steps:

a) To configure the access point for SE-Connect mode, enter this command:

config ap mode se-connect *Cisco_AP*

b) When prompted to reboot the access point, enter **Y.**
c) To verify the SE-Connect configuration status for the access point, enter this command:

show ap config {**802.11a** | **802.11b**} *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... CISCO_AP3500
...
Spectrum Management Information
        Spectrum Management Capable.............. Yes
        Spectrum Management Admin State.......... Enabled
        Spectrum Management Operation State...... Up
        Rapid Update Mode........................ Disabled
        Spectrum Expert connection............... Enabled
   Spectrum Sensor State.................. Configured (Error code = 0)
```

Step 4 On the Windows PC, access the Cisco Software Center from this URL:

http://www.cisco.com/cisco/software/navigator.html

Step 5 Click **Product > Wireless > Cisco Spectrum Intelligence** > **Cisco Spectrum Expert** > **Cisco Spectrum Expert Wi-Fi**, and then download the Spectrum Expert 4.0 executable (*.exe) file.

Step 6 Run the Spectrum Expert application on the PC.

Step 7 When the Connect to Sensor dialog box appears, enter the IP address of the access point, choose the access point radio, and enter the 16-byte network spectrum interface (NSI) key to authenticate. The Spectrum Expert application opens a TCP/IP connection directly to the access point using the NSI protocol.

Note The access point must be a TCP server listening on ports 37540 for 2.4 GHz and 37550 for 5 GHz frequencies. These ports must be opened for the spectrum expert application to connect to the access point using the NSI protocol.

Note On the controller GUI, the NSI key appears in the Network Spectrum Interface Key field (below the Port Number field) on the All APs > Details for page. To view the NSI key from the controller CLI, enter the **show ap config** {**802.11a** | **802.11b**} *Cisco_AP* command.

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.

Note You can establish up to three Spectrum Expert console connections per access point radio. The Number of Spectrum Expert Connections text box on the 802.11a/n/ac/ax (or 802.11b/g/n/ax) Cisco APs > Configure page of the controller GUI shows the number of Spectrum Expert applications that are currently connected to the access point radio.

Step 8 Verify that the Spectrum Expert console is connected to the access point by selecting the Slave Remote Sensor text box in the bottom right corner of the Spectrum Expert application. If the two devices are connected, the IP address of the access point appears in this text box.

Step 9 Use the Spectrum Expert application to view and analyze spectrum data from the access point.

Cisco Universal Small Cell 8x18 Dual-Mode Module

Cisco Universal Small Cell 8x18 Dual-Mode Module is an external module (4G/LTE) that can be plugged into the Cisco Aironet 3600I APs or Cisco Aironet 3700I APs. The following features are available:

- You can configure VLAN tagging for the external module's traffic for the following modes:

Mode	Native VLAN	Non-Native VLAN
FlexConnect Local Switching	Supported	Supported
Local Mode Central Switching	Supported	Supported

- The module can be powered up by the PoE+ power supply
- Co-existence detection and warning when Wi-Fi in 2.4 GHz and 3G/4G module are enabled
- The module's inventory details are available on the controller GUI at **Wireless** > **Access Points** > ***Access Point name*** > **Inventory**.
- Supported on the following Cisco Wireless Controller models:
  - Cisco 3504 Controller
  - Cisco 5520 Controller
  - Cisco 8540 Controller
  - Cisco Virtual Controller
- Supported on the following Cisco Access Point models:
  - Cisco Aironet 3700I AP

Restrictions

Cisco Universal Small Cell 8x18 Dual-Mode Modules are not supported on the following Cisco Access Point models:

- Cisco Aironet 3700E AP

For more information about Cisco Universal Small Cell 8x18 Dual-Mode modules, see http://www.cisco.com/c/en/us/support/wireless/universal-small-cell-8000-series/tsd-products-support-series-home.html.

This section contains the following subsections:

Configuring Cisco Universal Small Cell 8x18 Dual-Mode Module

Configuring Cisco Universal Small Cell 8x18 Dual-Mode Module (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs**.

Step 2 Click the AP name.
The **All APs > Details** page is displayed.

Step 3 In the **Advanced** tab, check or uncheck the **External Module Status** check box.

You might be prompted with a co-existence warning when Wi-Fi in 2.4-GHz and 3G/4G module are enabled.

Configuring Cisco Universal Small Cell 8x18 Dual-Mode Module (CLI)

Procedure

- Enable or disable the Cisco USC 8x18 Dual-Mode Module by entering this command:
  config ap module3G {**enable** | **disable**} *ap-name*

  You might be prompted with a co-existence warning when Wi-Fi in 2.4-GHz and 3G/4G module are enabled.

Configuring USC8x18 Dual-Mode Module in Different Scenarios

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Local Switching (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs**.

Step 2 Click the AP name.
The **All APs > Details** page is displayed.

Step 3 In the **FlexConnect** tab, check the **VLAN Support** check box and enter the number of the native VLAN on the remote network (such as 100) in the **Native VLAN ID** box.

Step 4 To enable FlexConnect Local Switching with VLAN ID that is other than 0:

a) Enable **FlexConnect Local Switching** under **External Module**.
b) Enter a value between 2 and 4096 in the **VLAN ID** box.
c) Click **Apply**.

Step 5 To enable FlexConnect local switching with VLAN ID equal to 0:
a) Enable **FlexConnect Local Switching** under **External Module**.
b) Click **Apply**.

Step 6 To remove the FlexConnect local switching per AP configuration, click **Remove AP Specific Config**.

Step 7 Save the configuration.

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Local Switching (CLI)

Procedure

- **config ap flexconnect module-vlan enable** *ap-name* —Enables FlexConnect local switching for external module with native VLAN
- **config ap flexconnect module-vlan remove** *ap-name*—Removes the AP specific external module VLAN configuration
- **config ap flexconnect module-vlan enable** *ap-name* **vlan** *vlan-id*—Enables FlexConnect local switching with non-native VLAN for the external module
- **show ap module summary** {*ap-name* | **all**}—Displays detailed information about the external module.
- **show ap inventory** {*ap-name* | **all**}—Displays information about the AP's inventory and the external module, if the module is present
- **show ap flexconnect module-vlan** *ap-name*—Displays status of FlexConnect local switching and VLAN ID value
- **show ap config general** *ap-name*—Displays information about the external module info, if the module is present.

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Group Local Switching (GUI)

Procedure

Step 1 Choose **Wireless** > **FlexConnect Groups**.

Step 2 Click **New**, enter the FlexConnect group name, and click **Apply**.

Step 3 On the **FlexConnect Groups > Edit** page, in the **FlexConnect APs** area, click **Add AP**.

Step 4 You can either select an AP from a list of APs associated with the controller or directly specify the Ethernet MAC address of the AP that is associated with the controller.

Step 5 Click **Add**.

Step 6 To enable FlexConnect Local Switching with VLAN ID:
a) Enable **FlexConnect Local Switching** under **External Module Configuration**.
b) Enter a value between 2 and 4096 in the **VLAN ID** box.
c) Click **Apply**.

Step 7 Save the configuration.

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Group Local Switching (CLI)

Procedure

- **config flexconnect group** *group-name* **module-vlan enable vlan** *vlan-id*—Enables FlexConnect local switching for the FlexConnect group
- **config flexconnect group** *group-name* **module-vlan disable**—Disables the FlexConnect local switching for the FlexConnect group
- **show flexconnect group detail** *group-name* **module-vlan**—Displays status of the FlexConnect local switching and VLAN ID in the group

Configuring USC8x18 Dual-Mode Module in Local Mode Central Switching (GUI)

Procedure

Step 1 Create a Remote LAN.

For instructions to create a remote LAN, see the *Configuring Remote LANs* chapter under *WLANs*.

Step 2 On the **WLANs > Edit** page, click the **Security** tab.

Step 3 In the **Layer 2** sub-tab, uncheck the **MAC Filtering** check box.

Note Remote LAN should be configured only with open security. 802.1X security is not supported.

Step 4 To see the current state of the 3G/4G client, choose **Monitor** > **Clients** to open the **Clients** page.

Step 5 Save the configuration.

Configuring USC8x18 Dual-Mode Module in Local Mode Central Switching (CLI)

Procedure

- Create a Remote LAN.

  For instructions to create a remote LAN, see the *Configuring Remote LANs* chapter under *WLANs*.

- **config interface 3g-vlan** *interface-name* {**enable** | **disable**}—Enables or disables the 3G/4G-VLAN interface
- **show interface detailed** *interface-name*—Displays status of the 3G/4G-VLAN flag
- **show client summary ip**—Displays status of the 3G/4G clients

LED States for Access Points

In a wireless LAN network where there are a large number of access points, it is difficult to locate a specific access point associated with the controller. You can configure the controller to set the LED state of an access point so that it blinks and the access point can be located. This configuration can be done in the wireless network on a global as well as per-AP level.

The LED state configuration at the global level takes precedence over the AP level.

This section contains the following subsections:

Configuring the LED State for Access Points in a Network Globally (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the **Global Configuration** page.

Step 2 Check the **LED state** check box.

Step 3 Choose **Enable** from the drop-down list adjacent to this check box.

Step 4 Click **Apply**.

Configuring the LED State for Access Point in a Network Globally (CLI)

Procedure

- Set the LED state for all access points associated with a controller by entering this command:

  config ap led-state {**enable** | **disable**} **all**

Configuring LED State on a Specific Access Point (GUI)

Procedure

Step 1 Choose **Wireless > Access Points > All APs** and then the name of the desired access point.

Step 2 Choose the **Advanced** tab to open the **All APs > Details for (Advanced)** page.

Step 3 Check the **LED state** check box.

Step 4 Choose **Enable** from the drop-down list adjacent to this text box.

Step 5 Click **Apply**.

Configuring LED State on a Specific Access Point (CLI)

Procedure

Step 1 Determine the ID of the access point for which you want to configure the LED state by entering this command:

show ap summary

Step 2 Configure the LED state by entering the following command:

config ap led-state {**enable** | **disable**} *Cisco_AP*

Configuring Flashing LEDs

Information About Configuring Flashing LEDs

Controller software enables you to flash the LEDs on an access point in order to locate it. All Cisco IOS lightweight access points support this feature.

Configuring Flashing LEDs (CLI)

Use these commands to configure LED flashing from the privileged EXEC mode of the controller:

1. Configure the LED flash for an AP by entering this command:

   config ap led-state flash {*seconds* | **indefinite** | **disable**} {*Cisco_AP*}

   The valid LED flash duration for the AP is 1 to 3600 seconds. You can also configure the LED to flash indefinitely or to stop flashing the LED.

2. Disable LED flash for an AP after enabling it by entering this command:

   config ap led-state flash disable *Cisco_AP*

   The command disables LED flashing immediately. For example, if you run the previous command (with the *seconds* parameter set to 60 seconds) and then disable LED flashing after only 20 seconds, the access point's LEDs stop flashing immediately.

3. Save your changes by entering this command:

   save config

4. Check the status of LED flash for the AP by entering this command:

   show ap led-flash *Cisco_AP*

   Information similar to the following appears:

```
(Cisco Controller)> show ap led-flash AP1040_46:b9
Led Flash..................................... Enabled for 450 secs, 425 secs left
```

Note The output of these commands is sent only to the controller console, regardless of whether the commands were entered on the console or in a TELNET/SSH CLI session.

Configuring LED Flash State on a Specific Access Point (GUI)

Procedure

Step 1 Choose **Wireless > Access Points > All APs** and then the name of the desired access point.

Step 2 Choose the **Advanced** tab to open the **All APs > Details for (Advanced)** page.

Step 3 In the **LED Flash State** section, select one of the following radio buttons:

- 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.

Step 4 Click **Apply**.

LED Brightness Settings

This section contains the following subsections:

Configuring LED Brightness Level for AP Globally (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the **Global Configuration** page.

Step 2 In the **General** section, check the **LED Brightlevel** check box.

Step 3 Enter the brightness value in the **LED Brightlevel** text box.

The range is between 1 and 8.

Step 4 Save the configuration.

Configuring LED Brightness Level on a Specific AP (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs** then click the name of the desired access point.

Step 2 Choose the **Advanced** tab to open the **All APs** > **Details** page.

Step 3 In the **LED Brightness** text box, enter the brightness level value.

The range is between 1 and 8.

Step 4 Save the configuration.

Configuring LED Brightness Level (CLI)

Procedure

- Configure the AP status LED brightness level globally or on a specific AP by entering this command:

  config ap led-brightlevel *brightlevel-range* {**all** | *ap-name*}

- View the brightness levels by entering this command:

  show ap led-brightlevel {**all** | *ap-name*}

Access Points with Dual-Band Radios

This section contains the following subsections:

Configuring Access Points with Dual-Band Radios (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Radios** > **Dual-Band Radios** to open the Dual-Band Radios page.

Step 2 Hover your cursor over the blue drop-down arrow of the AP and click **Configure**.

Step 3 Configure the Admin Status.

Step 4 Configure CleanAir Admin Status as one of the following:

- Enable
- Disable
- 5 GHz Only
- 2.4 GHz Only

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

What to do next

You can monitor the access points with dual-band radios by navigating to **Monitor** > **Access Points** > **Radios** > **Dual-Band Radios**.

Configuring Access Points with Dual-Band Radios (CLI)

Procedure

- Configure an access point with dual-band radios by entering this command:

  config 802.11-abgn {**enable** | **disable**} *ap-name*

- Configure the CleanAir features for an access point with dual-band radios by entering this command:

  config 802.11-abgn cleanair {**enable** | **disable**} *ap-name* **band** *2.4-or-5-GHz*

- Configure the dual band Rx-only radio features for an access point with dual-band radios by entering this command:

  config 802.11-rx-abgn {{**cleanair** {**enable** | **disable**}} | **enable** | **disable**} *ap-name*

Access Point Antenna Monitoring and Failure Detection

Having multiple antennas on the transmitter and receiver of APs results in better performance and reliability of the APs. Multiple antennas improve reception through the selection of the stronger signal or a combination of individual signals at the receiver. Therefore, detection of physical breakage of antennas is critical to the reliability of APs.

This feature is based on the signal strength delta across the antennas on the receiver. If the delta is more than the defined limit for a specific duration, the antenna is considered to have issues.

Configuring Access Point Antenna Monitoring and Failure Detection (CLI)

Procedure

- Enable or disable AP antenna monitoring and failure detection in all the APs, in a specific AP, or in a specific AP group by entering this command:

  config ap antenna monitoring {**all** | **ap-name** *ap-name* | **ap-group** *ap-group-name*} {**enable** | **disable**}

- Configure the RSSI delta threshold in all the APs, in a specific AP, or in a specific AP group by entering this command:

  config ap antenna monitoring {**all** | **ap-name** *ap-name* | **ap-group** *ap-group-name*} **rssi-failure-threshold** *value*

  The valid range of the RSSI failure threshold value is between 10 and 90. The default value is 40.

- Configure the weak RSSI threshold in all the APs, in a specific AP, or in a specific AP group by entering this command:

  config ap antenna monitoring {**all** | **ap-name** *ap-name* | **ap-group** *ap-group-name*} **weak-rssi** *value*

  The valid range of the weak RSSI threshold value is between 10 and 90. The default value is 60.

- Configure the detection time period in which to monitor the signal strength before a problem is flagged, in all the APs, in a specific AP, or in a specific AP group, by entering this command:

  config ap antenna monitoring {**all** | **ap-name** *ap-name* | **ap-group** *ap-group-name*} **detection-time** *value-in-minutes*

The valid range of the detection time is between 9 and 180 minutes. The default value is 12 minutes.

Calculating Ideal Configuration Values

To calculate the ideal configuration values for corresponding RSSI strong threshold and weak RSSI, we recommend that you first calculate the per-antenna RSSI for the corresponding AP. Use the **sho cont do 0/1 | i Last** command to know the per-antenna RSSI.

The following are the various ways in which the per-antenna RSSI can be calculated using the **sho cont do 0/1 | i Last** command:

Method	Description
Having all the antennas are connected	With this, you will know the lowest value of strong RSSI. This is the ideal weak RSSI. The default value is 60, but it can be in the range of 50 to 70.
Having all the antennas removed	
Having one, two, or three antennas removed	With this, you will know the RSSI difference between an antenna that is present and the one that is unavailable. This is the ideal RSSI strong threshold value. The default value is 40.

This feature gives accurate results only if you configure calculated values as described in this section.

Monitoring Access Point Antenna Monitoring and Failure Detection (CLI)

Procedure

- View the AP antenna monitoring and failure detection status on the controller CLI by entering this command:

  show ap config general *ap-name*

  The following is a sample output:

```
(Cisco Controller) >show ap config general AP58AC.78DC.C2F0


Cisco AP Identifier.............................. 49
Cisco AP Name.................................... AP58AC.78DC.C2F0
Country code..................................... Multiple Countries : AE,CA,US
Regulatory Domain allowed by Country............. 802.11bg:-ACE   802.11a:-ABCE
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 28:ac:18:dd:c1:f0
IP Address Configuration......................... DHCP
IP Address....................................... 209.165.200.225
IP NetMask....................................... 255.255.255.224
Gateway IP Addr.................................. 209.165.200.254
.
.
.
AP broken antenna detection - Status ............ Enabled (Global)
RSSI Failure Threshold .......................... 40

--More-- or (q)uit
Weak RSSI ....................................... 60
Detection Time .................................. 12
If any broken antenna?........................... ALL
```

```
Memory Type..................................... DDR3
Memory Size..................................... 1028096 KBytes
CPU Type.....................................  ARMv7 Processor rev 1 (v7l)
```

Note For every detection time period that you configure, the AP sends an IAPP message that carries the antenna condition. This is displayed in the controller trap messages, SNMP traps, and controller debug logs. The following is a sample trap message:

```
Broken Antenna Detection details for AP AP58AC.78DC.C2F0 received.
Antennas reporting weak signal – ALL
```

- View the AP antenna monitoring and failure detection status on the AP CLI by entering this command:

  show configuration

  The following is a sample output:

```
cisco-wave2-ap# show configuration

AP Name                     : AP58AC.78DC.C2F0
Admin State                 : Enabled
AP Mode                     : FlexConnect
AP Submode                  : Not Configured
Location                    : default location
Reboot Reason               : Reload command
.
.
AP Link LAG status          : Disabled
AP WSA Mode                 : Enabled
Vlan Interface              : Disabled

Broken antenna detection    : Enabled (Global)
RSSI Failure Threshold      : 40
Weak RSSI                   : 60
Detection Time              : 12
If any broken antenna?      : ALL
AP58AC.78DC.C2F0#
```

BSS Coloring and Spatial Reuse

The 802.11 Wi-Fi standard minimizes the chance of multiple devices interfering with one another by transmitting at the same time. This carrier-sense multiple access with collision avoidance (CSMA/CA) technology was based on static thresholds that allowed Wi-Fi devices to avoid interfering with each other on air. However, with increased density and number of Wi-Fi devices, these static thresholds often lead to CSMA/CA, causing devices to defer transmissions unnecessarily.

For example, if two devices associated with different Basic Service Set (BSS) can hear each transmissions from each other at relatively low signal strengths, each device has to defer its transmission when it receives a transmission from the other. But, if both devices were to transmit at the same time, it is likely that neither would cause enough interference at the other BSS receiver to cause reception failure for either transmission.

Devices today must demodulate packets to look at the MAC header in order to determine whether or not a received packet belongs to their own BSS. This process consumes power, which could have been saved if devices could quickly identify the BSS by looking at the PHY header alone, and subsequently drop packets that are from a different BSS. Before Wi-Fi 6, there was no provision for devices to do this.

The new 802.11ax (Wi-Fi 6) standard addresses both of the issues discussed above through the new BSS Coloring and Spatial Reuse mechanisms. BSS Coloring is a new provision that allows devices operating in the same frequency space to quickly distinguish between packets from their own BSS and packets from an Overlapping BSS (OBSS), by simply looking at the *BSS color* value contained in the HE PHY header. Spatial Reuse allows devices, in some cases, to transmit at the same time as OBSS packets they receive, instead of having to defer transmissions due to legacy interference thresholds. As every Wi-Fi 6 device understands the BSS color, it can be leveraged to increase power savings by dropping packets earlier, and to identify spatial reuse opportunities.

This section contains the following subsections:

BSS Coloring

BSS Coloring is a method to differentiate between BSS (APs and their clients) on the same RF channel. Wi-Fi 6 enables each AP radio to assign a value (from 1 to 63), known as the BSS color, to be included in the PHY header of all HE transmissions from devices in its BSS. With devices of each BSS transmitting a locally-unique color, a device can quickly and easily distinguish transmissions coming from its BSS from those of a neighboring BSS.

Guidelines

- This feature is not supported on Cisco Catalyst 9117 access points and access points that do not support 802.11ax radio
- Enable 802.11ax support on 2.4-GHz and 5-GHz radio bands in the Cisco Controller.

Configuring BSS Coloring Globally on a Radio Band (CLI)

Procedure

- Configure BSS Coloring for all access points on a radio band by entering this command:

  config {**802.11a** | **802.11b** } **11axSupport bss-color global** {**enable** | **disable** }

- View the BSS Coloring configuration for all access points on a radio band by entering this command:

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

Configuring BSS Color for a Specific Access Point (CLI)

Procedure

- Configure BSS Color for a specific access point radio by entering this command:

  config {**802.11a** | **802.11b** | **802.11-abgn** } **11axSupport bss-color ap** *ap-name* **enable** *bss-color-value*}

  The valid range for manually setting BSS Color on an access point radio is between 1 and 63.

- Disable BSS Color for a specific access point radio by entering this command:

config { **802.11a** | **802.11b** | **802.11-abgn** } **11axSupport bss-color ap** *ap-name* **disable**

- View the BSS Color configuration on a access point band by entering this command:

  show ap config { **802.11a** | **802.11b** | **802.11-abgn** } *ap-name*

- View the BSS Color configuration on a specific radio by entering this command:

  show ap config slot *radio-slot ap-name*

  The valid radio slot range is between 0 and 2.

- View the BSS Color configuration on all access point radios on the band by entering this command:

  show advanced { **802.11a** | **802.11b** | **802.11-abgn** } **summary**