Mesh Access Points

Introduction to Mesh

In Cisco IOS XE 17.6.1 Release, the Cisco Embedded Wireless Controller (EWC) runs on the Cisco Catalyst 9124AX Series outdoor access points, acting as a Root Access Point (RAP) in a mesh deployment. Mesh networking employs Cisco Aironet outdoor mesh access points along with Cisco Embedded Wireless Controller (EWC) to provide scalability, central management, and mobility between deployments. Control and Provisioning of Wireless Access Points (CAPWAP) protocol manages the connection of mesh access points to the network.

Access points within a mesh network operate in one of the following ways:

- Root access point (RAP)
- Mesh access point (MAP)

EWC works on RAPs. RAPs have wired connections, whereas MAPs have wireless connection to the controller. Mesh APs communicate with their parent and child mesh APs using wireless connections over the 802.11a/n radio backhaul. MAPs use the Cisco Adaptive Wireless Path Protocol (AWPP) to determine the best path through the other mesh access points to the controller. A mesh access point establishes AWPP link with a parent Mesh AP, which is already connected to the controller before starting CAPWAP discovery.

The wireless mesh terminates on two points on the wired network. The first location is where the root access point (RAP) is attached to the wired network, and where all bridged traffic connects to the wired network. The second location is where the CAPWAP controller connect to the wired network; this location is where the WLAN client traffic from the mesh network is connected to the wired network. The WLAN client traffic from CAPWAP is tunneled to Layer 2. Matching WLANs should terminate on the same switch VLAN on which the wireless controllers are co-located. The security and network configuration for each of the WLANs on the mesh depend on the security capabilities of the network to which the wireless controller is connected.

End-to-end security within the mesh network is supported by employing Advanced Encryption Standard (AES) encryption between wireless mesh access points and Wi-Fi Protected Access 2 (WPA2) clients. For connections to a mesh access point (MAP) wireless client, such as MAP-to-MAP and MAP-to-root access point, WPA2 is applicable.

In the new configuration model, the controller has a default mesh profile. This profile is mapped to the default AP-join profile, which is in turn is mapped to the default site tag. If you are creating a named mesh profile, ensure that these mappings are put in place, and the corresponding AP is added to the corresponding site-tag.

Note If you change the configuration for Security Mode, BGN, Client-Access, and Range change in mesh profile, the mesh APs will reload. In EWC, you can not reload the internal AP to an active EWC, automatically. You must reload the internal AP manually, after the standby EWC node begins to work after the reload.

From this release, mesh support is included in the Cisco Catalyst 9130AX Series Access Points. All traditional capabilities of mesh are included in the Cisco Catalyst 9130AX Series APs operating in Cisco IOS XE Dublin 17.12.1.

Scale Numbers

Cisco Catalyst 9124 Series Outdoor Access Points support a scale of 100 APs and 2000 clients.

Restrictions and Limitations

- The mesh feature is supported only in Cisco Catalyst 9124 series Access Points, for Cisco Embedded Wireless Controllers.
- EWC supports AP roaming between parent mesh APs within the same controller, only.
- In an EWC mesh topology, any FlexConnect EWC capable AP should be in the CAPWAP mode, when deployed as a child to a MAP, for extending wireless network. The controller will be spawned, if the AP is not in the CAPWAP mode.

Mesh Deployments

Following are the mesh deployments:

- **Wireless Bridging**: Wireless bridging can be point-to-point or point-to-multipoint. Wireless bridges extend the network over the air when a cable is not available. The over-the-air link between the RAP and MAP(s) is treated as a pipe. This type of deployment is usually with RAP and one level of MAP. There are no child MAPs present under the first level of MAP. SSIDs are not deployed.
  - **Point-to-Point Wireless Bridging**: In a point-to-point bridging scenario, a Cisco Catalyst 9124 Series Mesh AP can be used to extend a remote network by using the backhaul radio to bridge two segments of a switched network. This is fundamentally a wireless mesh network with one MAP and no WLAN clients. Just as in point-to-multipoint networks, client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access.
  - **Point-to-Multipoint**: In the point-to-multipoint bridging scenario, a RAP acting as a root bridge connects multiple MAPs as non-root bridges with their associated wired LANs. By default, this feature is disabled for all MAPs. If Ethernet bridging is used, you must enable it on the controller for the respective MAP and for the RAP.
- **Mesh with Wi-Fi Clients**: Mesh deployments with multilevel MAPs and wireless clients, for extending Wi-Fi network. In a Cisco wireless outdoor mesh network, multiple mesh access points comprise a network that provides secure, scalable outdoor wireless LAN.

MAC Authorization

You must enter the MAC address of an AP in the controller to make a MAP join the controller. The controller responds only to those CAPWAP requests from MAPs that are available in its authorization list. Remember to use the MAC address provided at the back of the AP.

MAC authorization for MAPs connected to the controller over Ethernet occurs during the CAPWAP join process. For MAPs that join the controller over radio, MAC authorization takes place when the corresponding AP tries to secure an adaptive wireless path protocol (AWPP) link with the parent MAP. The AWPP is the protocol used in Cisco mesh networks.

The Cisco Catalyst 9800 Series Wireless Controller supports MAC authorization internally as well as using an external AAA server.

Configuring MAC Authorization (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **AAA Advanced** > **Device Authentication**.

Step 2 Click **Add**.
The **Quick Step: MAC Filtering** window is displayed.

Step 3 In the **Quick Step: MAC Filtering** window, complete the following:

a) Enter the **MAC Address**.
b) Choose the **Attribute List Name** from the drop-down list.
c) Choose the **WLAN Profile Name** from the drop-down list.
d) Click **Apply to Device**.

Step 4 Choose **Configuration** > **Security** > **AAA** > **AAA Method List** > **Authorization**.

Step 5 Click **Add**.
The **Quick Step: AAA Authorization** window is displayed.

Step 6 In the **Quick Step: AAA Authorization** window, complete the following:

a) Enter the **Method List Name**.
b) Choose the **Type** from the drop-down list.
c) Choose the **Group Type** from the drop-down list.
d) Check the **Fallback to Local** check box.
e) Check the **Authenticated** check box.
f) Move the required servers from the **Available Server Groups** to the **Assigned Server Groups.**
g) Click **Apply to Device**.

Step 7 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 8 Click the mesh profile.
The **Edit Mesh Profile** window is displayed.

Step 9 Click the **Advanced** tab.

Step 10 In the **Security** settings, from the **Method** drop-down list, choose **EAP**.

Step 11 Choose the **Authentication Method** from the drop-down list.

Step 12 Choose the **Authorization Method** from the drop-down list.

Step 13 Click **Update & Apply to Device**.

Configuring MAC Authorization (CLI)

Follow the procedure given below to add the MAC address of a bridge mode AP to the controller.

Before you begin

- MAC filtering for bridge mode APs are enabled by default on the controller. Therefore, only the MAC address need to be configured. The MAC address that is to be used is the one that is provided at the back of the corresponding AP.
- MAC authorization is supported internally, as well as using an external AAA server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**username** *user-name* **Example:** `Device(config)# username username1`	Configures user name authentication for MAC filtering where username is MAC address.
Step 3	**aaa authorization credential-download** *method-name* **local** **Example:** `Device(config)# aaa authorization credential-download list1 local`	Sets an authorization method list to use local credentials.
Step 4	**aaa authorization credential-download** *method-name* **radius group** *server-group-name* **Example:** `Device(config)# aaa authorization credential-download auth1 radius group radius-server-1`	Sets an authorization method list to use a RADIUS server group.
Step 5	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 6	**method authorization** *method-name* **Example:**	Configures the authorization method for mesh AP authorization.

	Command or Action	Purpose
	`Device(config-wireless-mesh-profile)# method authorization auth1`	

Preshared Key Provisioning

Customers with mesh deployments can see their MAPs moving out of their network and joining another mesh network when both these mesh deployments use AAA with wild card MAC filtering to allow the association of MAPs. Since MAPs might use EAP-FAST, this cannot be controlled because a security combination of MAC address and type of AP is used for EAP, and no controlled configuration is available. The preshared key (PSK) option with a default passphrase also presents a security risk.

This issue is prominently seen in overlapping deployments of two service providers when the MAPs are used in a moving vehicle (public transportation, ferry, ship, and so on.). This way, there is no restriction on MAPs to remain with the service providers' mesh network, and MAPs can get hijacked or getting used by another service provider's network and cannot serve the intended customers of the original service providers in the deployment.

The PSK key provisioning feature enables a provisionable PSK functionality from the controller which helps make a controlled mesh deployment and enhance MAPs security beyond the default one. With this feature the MAPs that are configured with a custom PSK, will use the PSK key to do their authentication with their RAPs and controller.

Configuring PSK Provisioning (GUI)

To configure PSK provisioning, follows these steps:

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** .

Step 2 Click the **Global Config** tab.

Step 3 In the **Security** settings, check the **PSK Provisioning** check box and complete the following steps:

a) Choose the **PSK Inuse Index** from the numbers in the drop-down list.
b) In the **Keys Configuration** settings, click the add icon '+' to configure the keys.
c) Choose the **Key** from the drop-down list.
d) Enter the **Name** and the **Description** of the key that is to be configured.
e) Choose the **Password Type** as **UNENCRYPTED** or **AES Encrypted**.
f) Click **Apply**. The key is listed in the list of configured keys.

Step 4 Check the **Default PSK** check box.

Step 5 Click **Apply**.

Configuring PSK Provisioning (CLI)

When PSK provisioning is enabled, the APs join with default PSK initially. After that PSK provisioning key is set, the configured key is pushed to the newly joined AP.

Follow the procedure given below to configure a PSK:

Before you begin

The provisioned PSK should have been pushed to all the APs that are configured with PSK as mesh security.

Note

- PSKs are saved across reboots in the controller as well as on the corresponding mesh AP.
- A controller can have total of five PSKs and one default PSK.
- A mesh AP deletes its provisioned PSK only on factory reset.
- A mesh AP never uses the default PSK after receiving the first provisioned PSK.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh security psk provisioning** **Example:** `Device(config)# wireless mesh security psk provisioning`	Configures the security method for wireless as PSK. **Note** The provisioned PSK is pushed only to those APs that are configured with PSK as the mesh security method.
Step 3	**wireless mesh security psk provisioning key** *index* {**0** | **8**} *pre-shared-key description* **Example:** `Device(config)# wireless mesh security psk provisioning key 1 0 secret secret-key`	Configures a new PSK for mesh APs.
Step 4	**wireless mesh security psk provisioning default-psk** **Example:** `Device(config)# wireless mesh security psk provisioning default-psk`	Enables default PSK-based authentication.
Step 5	**wireless mesh security psk provisioning inuse** *index*	Specifies the PSK to be actively used.

	Command or Action	Purpose
	Example: `Device(config)# wireless mesh security psk provisioning inuse 1`	**Note** You should explicitly set the in-use key index in the global configuration pointing to the PSK index.

EAP Authentication

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally on the controller. It is designed for use in remote offices that want to maintain connectivity with wireless clients when the backend system gets disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, which in turn, removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users. Local EAP supports only the EAP-FAST authentication method for MAP authentication between the controller and wireless clients.

Local EAP uses an LDAP server as its backend database to retrieve user credentials for MAP authentication between the controller and wireless clients. An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user.

Note If RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if RADIUS servers are not found, timed out, or were not configured.

EAP Authentication with LSC

Locally significant certificate-based (LSC-based) EAP authentication is also supported for MAPs. To use this feature, you should have a public key infrastructure (PKI) to control certification authority, define policies, validity periods, and restrictions and usages on the certificates that are generated, and get these certificates installed on the APs and controller.

After these customer-generated certificates or LSCs are available on the APs and controller, the devices can start using these LSCs, to join, authenticate, and derive a session key.

LSCs do not remove any preexisting certificates from an AP. An AP can have both LSC and manufacturing installed certificates (MIC). However, after an AP is provisioned with an LSC, the MIC certificate is not used during boot-up. A change from an LSC to MIC requires the corresponding AP to reboot.

The controller also supports mesh security with EAP authentication to a designated server in order to:

- Authenticate the mesh child AP
- Generate a master session key (MSK) for packet encryption.

Bridge Group Names

Bridge group names (BGNs) control the association of MAPs to the parent mesh AP. 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). BGN is a string comprising a maximum of 10 characters.

A BGN of *NULL VALUE* is assigned by default during manufacturing. Although not visible to you, it allows a MAP to join the network prior to your assignment of your network-specific BGN.

If you have two RAPs in your network in the same sector (for more capacity), we recommend that you configure the two RAPs with the same BGN, but on different channels.

When Strict Match BGN is enabled on a MAP, it will scan ten times to find a matching BGN parent. After ten scans, if the AP does not find the parent with matching BGN, it will connect to the nonmatched BGN and maintain the connection for 15 minutes. After 15 minutes, the AP will again scan ten times, and this cycle continues. The default BGN functionalities remain the same when Strict Match BGN is enabled.

In Cisco Catalyst 9800 Series Wireless Controller, the BGN is configured on the mesh profile. Whenever a MAP joins the controller, the controller pushes the BGN that is configured on the mesh profile to the AP.

Note In the EWC HA pair, switchover happens if you change the BGN configuration. If you remove the configured BGN from the mesh profile, a switchover is triggered.

Preferred Parent Selection

The preferred parent for a MAP enables you to enforce a linear topology in a mesh environment. With this feature, you can override the Adaptive Wireless Path Protocol-defined (AWPP-defined) parent selection mechanism and force a MAP to go to a preferred parent.

For Cisco Wave 1 APs, when you configure a preferred parent, ensure that you specify the MAC address of the actual mesh neighbor for the desired parent. This MAC address is the base radio MAC address that has the letter "f" as the final character. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:0f as the preferred parent.

```
Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:0f
```

For Cisco Wave 2 APs, when you configure a preferred parent, the MAC address is the base radio MAC address that has "0x11" added to the last two characters. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:11 as the preferred parent.

```
Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:11
```

Configuring a Bridge Group Name (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Click **Add**.

Step 3 In the **Advanced** tab, under the **Bridge Group** settings, enter the **Bridge Group Name**.

Step 4 Under the **Bridge Group** settings, check the **Strict Match** check box to enable the feature. When Strict Match BGN is enabled on a MAP, it scans ten times to find a matching BGN parent.

Step 5 Click **Apply to Device**.

Configuring a Bridge Group Name (CLI)

- If a bridge group name (BGN) is configured on a mesh profile, whenever a MAP joins the controller, it pushes the BGN configured on the mesh profile to the AP.
- Whenever a mesh AP moves from AireOS controller to the Cisco Catalyst 9800 Series Wireless Controller, the BGN configured on the mesh profile is pushed to that AP and stored there.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**bridge-group name** *bridge-grp-name* **Example:** `Device(config-wireless-mesh-profile)# bridge-group name bgn1`	Configures a bridge group name.
Step 4	**bridge-group strict-match** **Example:** `Device(config-wireless-mesh-profile)# bridge-group strict-match`	Configures bridge group strict matching.

Mesh Backhaul at 2.4 GHz and 5 GHz

A backhaul is used to create only the wireless connection between MAPs. The backhaul interface is 802.11a/n/ac/g depending upon the AP. The default backhaul interface is 5-GHz. The rate selection is important for effective use of the available radio frequency spectrum. The rate can also affect the throughput of client devices. (Throughput is an important metric used by industry publications to evaluate vendor devices.)

Mesh backhaul is supported at 2.4-GHz and 5-GHz. However, in certain countries it is not allowed to use mesh network with a 5-GHz backhaul network. The 2.4-GHz radio frequencies allow you to achieve much

larger mesh or bridge distances. When a RAP gets a slot-change configuration, it gets propagated from the RAP to all its child MAPs. All the MAPs get disconnected and join the new configured backhaul slot.

Configuring Mesh Backhaul (CLI)

This section describes how to configure mesh backhaul at 2.4 GHz.

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap_name* **mesh backhaul radio dot11** *24ghz* **Example:** `Device # ap name test-ap mesh backhaul radio dot11 24ghz`	Changes the mesh backhaul to 2.4 GHz.

Information About Mesh Backhaul RRM

Root access points (RAPs) choose backhaul channels to operate in mesh networks. Until Cisco IOS XE Cupertino 17.8.1, this operation occured by an explicit configuration, a least congested scan during RAP boot time, during the initial radio resource management (RRM) run without mesh access points (MAPs) connected, or a backhaul channel that was chosen at random. As a result, a poor backhaul channel selection resulted in poor performance.

From Cisco IOS XE Cupertino 17.9.1 onwards, RRM DCA is run on mesh backhaul, in auto mode, in FlexConnect or centralized networks. For APs that do not have dedicated (RHL) radios, DCA is triggered by running commands in the privilege EXEC mode.

RRM continuously evaluates the channel conditions to ensure that the network utilizes the least congested channels. The network uses the transmission static power if it is configured, or falls back to the default level. This is supported on APs that have dedicated radios to scan channel conditions, without any user perceptible interruption to the mesh network traffic.

In the mesh backhaul RRM feature, the RRM DCA decides all the downlink channels in a steady network. However, if an AP detects a change in its uplink roam or radar detection response, the AP chooses the best downlink to converge faster.

Note APs choosing the best possible downlink is limited to serial backhaul enabled APs only.

Configuring RRM Channel Assignment for an Access Point

To trigger RRM DCA for an AP, complete the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco-ap-name* **dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel update mesh** **Example:** `Device# ap name Cisco-ap-name dot11 5ghz rrm channel update mesh`	Triggers RRM DCA for the specific AP.

Configuring RRM Channel Assignment for Root Access Points Globally

Before you begin

Ensure that you have configured RRM for mesh backhaul before RRM DCA is triggered.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh backhaul rrm** **Example:** `Device(config)# wireless mesh backhaul rrm`	Configures RRM for mesh backhaul.
Step 3	(Optional) **wireless mesh backhaul rrm auto-dca** **Example:** `Device(config)# wireless mesh backhaul rrm auto-dca`	Configures auto DCA for RF Application Specific Integrated Circuit (ASIC) integrated RAPs.

To configure the initial channel assignment of the RAP in priviliged EXEC mode through RRM, and to initiate channel selection for each bridge group, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enters privileged EXEC mode.

	Command or Action	Purpose
	`Device# enable`	
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel-update mesh** **Example:** `Device# ap dot11 5ghz rrm channel-update mesh`	Initiates update of the 802.11, 802.11a, or 802.11b channel selection for every mesh Cisco AP.
Step 3	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel-update mesh bridge-group** *bridge-group-name* **Example:** `Device# ap dot11 5ghz rrm channel-update mesh bridge-group cisco-bridge-group`	Initiates update of the 802.11, 802.11a, or 802.11b channel selection for mesh AP in the bridge group.

Verifying the RRM DCA Status

To view the status of the DCA that is run for mesh APs, run the following command:

```
Device# show ap name Cisco-AP config general | inc Mesh
Mesh profile name                               : default-mesh-profile
Mesh DCA Run Status:                            : Not Running
Last Mesh DCA Run                               : 02/07/2022 01:21:56
```

To verify the status of the last DCA run per radio, run the following command:

```
Device# show wireless mesh rrm dca status
```

Dynamic Frequency Selection

To protect the existing radar services, the regulatory bodies require that devices that have to share the newly opened frequency sub-band behave in accordance with the Dynamic Frequency Selection (DFS) protocol. DFS dictates that in order to be compliant, a radio device must be capable of detecting the presence of radar signals. When a radio detects a radar signal, the radio should stop transmitting for at least 30 minutes to protect that service. The radio should then select a different channel to transmit on, but only after monitoring it. If no radar is detected on the projected channel for at least one minute, the new radio service device can begin transmissions on that channel. The DFS feature allows mesh APs to immediately switch channels when a radar event is detected in any of the mesh APs in a sector.

Configuring Dynamic Frequency Selection (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 2 Click **Add**.
The **Add Mesh Profile** window is displayed.

Step 3 In the **Add Mesh Profile** window, click the **General** tab.

Step 4 Enter a profile name.

Step 5 Check the **Full sector DFS status** check box to enable dynamic frequency selection.

Step 6 Click **Apply to Device**.

Configuring Dynamic Frequency Selection (CLI)

DFS specifies the types of radar waveforms that should be detected along with certain timers for an unlicensed operation in the DFS channel.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**full-sector-dfs** **Example:** `Device(config-wireless-mesh-profile)# full-sector-dfs`	Enables DFS. **Note** DFS functionality allows a MAP that detects a radar signal to transmit that up to the RAP, which then acts as if it has experienced radar and moves the sector. This process is called the coordinated channel change. The coordinated channel change is always enabled for Cisco Wave 2 and the later versions. The coordinated channel change can be disabled only for Cisco Wave 1 APs.

Country Codes

Controllers and APs are designed for use in many countries having varying regulatory requirements. The radios within the APs are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

In certain countries, there is a difference in the following for indoor and outdoor APs:

- Regulatory domain code
- Set of channels supported
- Transmit power level

Intrusion Detection System

The Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/CIPS) instructs controllers to block certain clients from accessing a wireless network when attacks involving these clients are detected in Layer 3 through Layer 7. This system offers significant network protection by helping to detect, classify, and stop threats, including worms, spyware or adware, network viruses, and application abuse.

Configuring the Intrusion Detection System (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 2 Click **Add**.
The **Add Mesh Profile** window is displayed.

Step 3 In the **Add Mesh Profile** window, click the **General** tab.

Step 4 Enter a profile name.

Step 5 Check the **IDS (Rogue/Signature Detection)** check box to enable the Intrusion Detection System.

Step 6 Click **Apply to Device**.

Configuring the Intrusion Detection System (CLI)

When enabled, the intrusion detection system generates reports for all the traffic on the client access. However, this is not applicable for the backhaul traffic.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.

	Command or Action	Purpose
Step 3	**ids** **Example:** `Device(config-wireless-mesh-profile)# ids`	Configures intrusion detection system reporting for mesh APs.

Mesh Interoperability Between Controllers

Interoperability can be maintained between AireOS and the Cisco Catalyst 9800 Series Wireless Controller with the following support:

- MAPs can join an AireOS controller through a mesh network formed by APs connected to a Cisco Catalyst 9800 Series Wireless Controller.
- MAPs can join a Cisco Catalyst 9800 Series Wireless Controller through a mesh network formed by APs connected to as AireOS controller.
- MAP roaming is supported between parent mesh APs connected to AireOS and the Cisco Catalyst 9800 Series Wireless Controller by using PMK cache.

Note For seamless interoperability, AireOS controller and the Cisco Catalyst 9800 Series Wireless Controller should be in the same mobility group and use the image versions that support IRCM.

Mesh Convergence

Mesh convergence allows MAPs to reestablish connection with the controller, when it loses backhaul connection with the current parent. To improve the convergence time, each mesh AP maintains a subset of channels that is used for future scan-seek and to identify a parent in the neighbor list subset.

The following convergence methods are supported.

Table 1: Mesh Convergence

Mesh Convergence	Parent Loss Detection / Keepalive Timers
Standard	21 / 3 seconds
Fast	7 / 3 seconds
Very Fast	4 / 2 seconds
Noise-tolerant-fast	21 / 3 seconds

Noise-Tolerant Fast

Noise-tolerant fast detection is based on the failure to get a response for an AWPP neighbor request, which evaluates the current parent every 21 seconds in the standard method. Each neighbor is sent a unicast request every 3 seconds along with a request to the parent. Failure to get a response from the parent initiates either a roam if neighbors are available on the same channel or a full scan for a new parent.

Configuring Mesh Convergence (CLI)

This section provides information about how to configure mesh convergence.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Creates a mesh profile.
Step 3	**convergence {fast | noise-tolerant-fast | standard | very-fast}** **Example:** `Device(config-wireless-mesh-profile)# convergence fast`	Configures mesh convergence method in a mesh profile.

Ethernet Bridging

For security reasons, the Ethernet port on all the MAPs are disabled by default. They can be enabled only by configuring Ethernet bridging on the root and its respective MAP.

Both tagged and untagged packets are supported on secondary Ethernet interfaces.

In a point-to-point bridging scenario, a Cisco Aironet 1500 Series MAP can be used to extend a remote network by using the backhaul radio to bridge multiple segments of a switched network. This is fundamentally a wireless mesh network with one MAP and no WLAN clients. Just as in point-to-multipoint networks, client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access. To use an Ethernet-bridged application, enable the bridging feature on the RAP and on all the MAPs in that sector.

Ethernet bridging should be enabled for the following scenarios:

- Use mesh nodes as bridges.
- Connect Ethernet devices, such as a video camera on a MAP using its Ethernet port.

Note Ensure that Ethernet bridging is enabled for every parent mesh AP taking the path from the mesh AP to the controller.

In a mesh environment with VLAN support for Ethernet bridging, the secondary Ethernet interfaces on MAPs are assigned a VLAN individually from the controller. All the backhaul bridge links, both wired and wireless, are trunk links with all the VLANs enabled. Non-Ethernet bridged traffic, as well as untagged Ethernet bridged traffic travels along the mesh using the native VLAN of the APs in the mesh. It is similar for all the traffic to and from the wireless clients that the APs are servicing. The VLAN-tagged packets are tunneled through AWPP over wireless backhaul links.

VLAN Tagging for MAP Ethernet Clients

The backhaul interfaces of mesh APs are referred to as primary interfaces, and other interfaces are referred to as secondary interfaces.

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).

Configuring Ethernet Bridging (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Click **Add**.

Step 3 In **General** tab, enter the **Name** of the mesh profile.

Step 4 In the **Advanced** tab, check the **VLAN Transparent** check box to enable VLAN transparency.

Step 5 In **Advanced** tab, check the **Ethernet Bridging** check box.

Step 6 Click **Apply to Device**.

Configuring Ethernet Bridging (CLI)

The Ethernet port on the MAPs are disabled by default. It can be enabled only by configuring Ethernet bridging on the Root AP and the other respective MAPs.

Ethernet bridging can be enabled for the following scenarios:

- To use the mesh nodes as bridges.
- To connect Ethernet devices, such as a video camera, on a MAP using the MAP's Ethernet port.

Before you begin

- Ensure that you configure the following commands under the mesh profile configuration for Ethernet bridging to be enabled:

- **ethernet-bridging**: Enables the Ethernet Bridging feature on an AP.
- **no ethernet-vlan-transparent**: Makes the wireless mesh bridge VLAN aware. Allows VLAN filtering with the following AP command: **[no] mesh ethernet** {**0** | **1** | **2** | **3**} **mode trunk vlan allowed**.

Note If you wish to have all the VLANs bridged (where bridge acts like a piece of wire), then you must enable VLAN transparency, which allows all VLANS to pass. If you choose to use VLAN transparent mode, it is best to filter the VLANS on the wired side of the network to avoid unnecessary traffic from flooding the network.

- The switch port to which the Root AP is connected should be configured as the trunk port for Ethernet bridging to work.
- For Bridge mode APs, use the **ap name** *name-of-rap* **mesh vlan-trunking native** *vlan-id* command to configure a trunk VLAN on the corresponding RAP. The Ethernet Bridging feature will not be enabled on the AP without configuring this command.
- For Flex+Brigde APs, configure the native VLAN ID under the corresponding flex profile.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode access** *vlan-id* **Example:** `Device# ap name ap1 mesh ethernet 1 mode access 21`	Configures the Ethernet port of the AP and sets the mode as trunk.
Step 3	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode trunk vlan** *vlan-id* **Example:** `Device# ap name ap1 mesh ethernet 1 mode trunk vlan native 21`	Sets the native VLAN for the trunk port.
Step 4	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode trunk vlan allowed** *vlan-id* **Example:** `Device# ap name ap1 mesh ethernet 1 mode trunk vlan allowed 21`	Configures the allowed VLANs for the trunk port. Permits VLAN filtering on an ethernet port of any Mesh or Root Access Point. Active only when VLAN transparency is disabled in the mesh profile.

Mesh Daisy Chaining

Mesh APs have the capability to *daisy chain* APs when they function as MAPs. The *daisy chained* MAPs can either operate the APs as a serial backhaul, allowing different channels for uplink and downlink access, thus improving backhaul bandwidth, or extend universal access. Extending universal access allows you to connect a local mode or FlexConnect mode Mesh AP to the Ethernet port of a MAP, thus extending the network to provide better client access.

Daisy chained APs must be cabled differently depending on how the APs are powered. If an AP is powered using DC power, an Ethernet cable must be connected directly from the LAN port of the Primary AP to the PoE in a port of the Subordinate AP.

The following are the guidelines for the daisy chaining mode:

- Primary MAP should be configured as mesh AP.
- Subordinate MAP should be configured as root AP.
- Daisy chaining should be enabled on both primary and subordinate MAP.
- Ethernet bridging should be enabled on all the APs in the Bridge mode. Enable Ethernet bridging in the mesh profile and map all the bridge mode APs in the sector to the same mesh profile.
- VLAN support should be enabled on the wired root AP, subordinate MAP, and primary MAP along with proper native VLAN configuration.

Restrictions for Mesh Ethernet Daisy Chaining

- This feature is applicable to the Cisco Industrial Wireless 3702 AP and Cisco Catalyst 9124 Series APs.
- This feature is applicable to APs operating in Bridge mode and Flex+Bridge mode only.
- In Flex+Bridge mode, if local switching WLAN is enabled, the work group bridge (WGB) multiple VLAN is not supported.
- To support the Ethernet daisy chain topology, you must not connect the Cisco Industrial Wireless 3702 PoE out port to other Cisco Industrial Wireless 3702 PoE in the port, and the power injector must be used as power supply for the AP.
- The network convergence time increases when the number of APs increase in the chain.
- Any EWC capable AP which is part of daisy chaining and has been assigned the RAP role, must be in CAPWAP mode (ap-type capwap).

Prerequisites for Mesh Ethernet Daisy Chaining

- Ensure that you have configured the AP role as root AP.
- Ensure that you have enabled Ethernet Bridging and Strict Wired Uplink on the corresponding AP.
- Ensure that you have disabled VLAN transparency.

- To enable VLAN support on each root AP for bridge mode APs, use the **ap name** *name-of-rap* **mesh vlan-trunking [native]** *vlan-id* command to configure a trunk VLAN on the corresponding RAP.
- To enable VLAN support on each root AP, for Flex+Bridge APs, you must configure the native VLAN ID under the corresponding flex profile.
- Ensure that you use a 4-pair cables that support 1000 Mbps. This feature does not work properly with 2-pair cables supporting 100 Mbps.

Configuring Mesh Ethernet Daisy Chaining (CLI)

The following section provides information about how to configure the Mesh Ethernet Daisy Chaining feature on a mesh AP.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile default-ap-profile** **Example:** `Device(config)# ap profile default-ap-profile`	Specifies an AP profile.
Step 3	**ssid broadcast persistent** **Example:** `Device(config-ap-profile)# ssid broadcast persistent`	Configures persistent SSID broadcast and ensures strict wired uplink. RAP will not switch to wireless backhaul when you configure this command.

Multicast Over Mesh Ethernet Bridging Network

Mesh multicast modes determine how bridging-enabled APs such as MAP and RAP, send multicast packets among Ethernet LANs within a mesh network. Mesh multicast modes manage only non-CAPWAP multicast traffic. CAPWAP multicast traffic is governed by a different mechanism.

Different mesh multicast modes are available to manage multicast and broadcast packets on all MAPs. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

The mesh multicast modes are:

- Regular mode: Regular mode for multicast is not supported on Cisco Catalyst 9124 Series Outdoor Access Points on EWC.
- In-only mode: Multicast packets received from the Ethernet by a MAP are forwarded to the corresponding RAP's Ethernet network. No additional forwarding occurs, which ensures that non-CAPWAP multicasts

received by the RAP are not sent back to the MAP Ethernet networks within the mesh network (their point of origin), and MAP to MAP multicasts do not occur because such multicasts are filtered out.

- In-out mode: The RAP and MAP both multicast but in a different manner.
  - If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP over Ethernet, and the MAP-to-MAP packets are filtered out of the multicast.
  - If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks. When the in-out mode is in operation, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.

Configuring Multicast Modes Over Mesh (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 2 Click **Add**.
The **Add Mesh Profile** window is displayed.

Step 3 In the **Add Mesh Profile** window, click the **General** tab.

Step 4 Enter a profile name.

Step 5 Choose one of the following **Multicast Modes**, from the drop-down list:

a) **Regular**: In this mode, data is multicast across the entire mesh network and all its segments by bridging-enabled RAP and MAP.

b) **In**: In this mode, the multicast packets received from the Ethernet by a MAP are forwarded to the corresponding RAP's Ethernet network.

c) **In-Out**: In this mode, both RAP and MAP multicast but in a different manner.

Step 6 Click **Apply to Device**.

Configuring Multicast Modes over Mesh

- If multicast packets are received at a MAP over Ethernet, they are sent to the RAP. However, they are not sent to other MAPs. MAP-to-MAP packets are filtered out of the multicast.
- If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks.
- The *in-out* mode is the default mode. When this *in-out* mode is in operation, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment, and then sent back into the network.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**multicast** {**in-only** | **in-out** | **regular**} **Example:** `Device(config-wireless-mesh-profile)# multicast regular`	Configures mesh multicast mode.

Radio Resource Management on Mesh

The Radio Resource Management (RRM) software embedded in the controller acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables the controller to continually monitor the associated lightweight APs for information on traffic load, interference, noise, coverage, and other nearby APs:

The RRM measurement in the mesh AP backhaul is enabled based on the following conditions:

- Mesh AP has the Root AP role.
- Root AP has joined using Ethernet link.
- Root AP is not serving any child AP.

Configuring RRM on Mesh Backhaul (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Global Config**.

Step 2 In the **Backhaul** section, check the **RRM** check box to enable radio resource management on mesh.

Step 3 Click **Apply**.

Configuring RRM on Mesh Backhaul (CLI)

The RRM measurement in the mesh AP backhaul is enabled based on the following conditions:

- Mesh AP has the Root AP role.

- Root AP has joined using an Ethernet link.
- Root AP is not serving any child AP.

Note After RRM is enabled on the mesh backhaul, the RRM noise information reported by the APs is only available for the RAP that has joined over an Ethernet link and which has no child MAPs connected.

Follow the procedure given below to enable RRM in the mesh backhaul:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh backhaul rrm** **Example:** `Device(config)# wireless mesh backhaul rrm`	Configures RRM on the mesh backhaul.

Mesh Leaf Node

You can configure a MAP with lower performance to work only as a leaf node. When the mesh network is formed and converged, the leaf node can only work as a child MAP, and cannot be selected by other MAPs as a parent MAP, thus ensuring that the wireless backhaul performance is not downgraded.

Configuring the Mesh Leaf Node (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.
Step 2 Click the Access Point.
Step 3 In the **Mesh** tab, check the **Block Child** check box.
Step 4 Click **Update & Apply to Device**.

Configuring the Mesh Leaf Node (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **mesh block-child** **Example:** `Device# #ap name ap1 mesh block-child`	Sets the AP to work only as a leaf node. This AP cannot be selected by other MAPs as a parent MAP. **Note** Use the **no** form of this command to change it to a regular AP.

Flex+Bridge Mode

Flex+Bridge mode is used to enable FlexConnect capabilities on mesh (bridge mode) APs. Mesh APs inherit VLANs from the root AP that is connected to it.

Any EWC capable AP in Flex mode connected to a MAP, should be in CAPWAP mode (AP-type CAPWAP).

You can enable or disable VLAN trunking and configure a native VLAN ID on each AP for any of the following modes:

- FlexConnect
- Flex+Bridge (FlexConnect+Mesh)

Backhaul Client Access

When Backhaul Client Access is enabled, it allows wireless client association over the backhaul radio. The backhaul radio can be a 2.4-GHz or 5-GHz radio. This means that a backhaul radio can carry both backhaul traffic and client traffic.

When Backhaul Client Access is disabled, only backhaul traffic is sent over the backhaul radio, and client association is performed only over the access radio.

Note Backhaul Client Access is disabled by default. After the Backhaul Client Access is enabled, all the MAPs, except subordinate AP and its child APs in daisy-chained deployment, reboot.

Configuring Backhaul Client Access (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Choose a profile.

Step 3 In **General** tab, check the **Backhaul Client Access** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Backhaul Client Access (CLI)

Note Backhaul client access is disabled by default. After it is enabled, all the MAPs, except subordinate AP and its child APs in daisy-chained deployment, reboot.

Follow the procedure given below to enable backhaul client access on a mesh profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**client-access** **Example:** `Device(config-wireless-mesh-profile)# client-access`	Configures backhaul with client access AP.

Information About Background Scanning and MAP Fast Ancestor Find Mode

Cisco mesh access points (MAPs) are interconnected over wireless links in a tree topology. A MAP that is connected to a network through the Ethernet uplink is the root MAP, which is also known as a root access point (RAP). Adaptive Wireless Path Protocol (AWPP) is used to form the tree topology and maintain that

topology. When a MAP comes up, it tries to look for another MAP (parent) to join and reach the gateway through a RAP. The same happens when a MAP loses connectivity with its existing parent. This procedure is known as mesh tree convergence.

A child MAP maintains uplink with its parent using the AWPP adjacency request/response messages that act as keepalive. If there is a consecutive loss of response messages, a parent is declared to be lost and the child MAP tries to find a new parent. A MAP maintains a list of neighbors of the current ON channel, and when the AP loses its current parent, it roams to the next best potential neighbor. If no other neighbors are found, the AP scans or seeks across all the channels or subset channels to find a parent. This is time consuming.

With the help of the Background Scanning feature, the AP avoids searching for a parent across the channel set by scanning or seeking. This feature helps the child MAP to be updated about its neighbors across all the channels, helps to switch to a neighbor of any channel, and uses that neighbor as its next parent for uplink.

Background scanning allows MAPs to save time during the scan-and-seek phase while looking for a new parent, but it does not save time on the authentication to the parent.

Enabling the MAP Fast Ancestor Finding feature enables a novel method to reduce the need for sending or receiving beacons at the network formation, while starting or deploying a new mesh network.

Note

- The Background Scanning and MAP Fast Ancestor Finding feature support in Cisco IOS XE Dublin 17.11.1, is not compatible with the legacy Background Scanning feature that is supported in the Cisco Wave 1 APs.
- When you enable Background Scanning on the APs that are not equipped with RHL radio, a performance penalty is imposed in terms of the bandwidth available in the backhaul. This performance penalty is high at system startup and lower after the system reaches the steady-state.

Configuring AP Fast Ancestor Find Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 2 Click **Add**.
The **Add Mesh Profile** window is displayed.

Step 3 In the **Add Mesh Profile** window, click the **General** tab.

Step 4 In the **Name** field, enter the mesh profile name.

Step 5 In the **Description** field, enter a description for the mesh profile.

Step 6 Check the **MAP Fast Ancestor Find** check box to enable a MAP (child) to synchronize with any neighbor MAP (parent) across all channels.

Step 7 Click **Apply to Device** to save the configuration.

Configuring Background Scanning and MAP Fast Ancestor Find Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device# wireless profile mesh default-mesh-profile`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**background-scanning** **Example:** `Device(config-wireless-mesh-profile)# background-scanning`	Configures background scanning in mesh deployments. **Note** In Cisco Catalyst 9124 Series Access Points, a dedicated RF ASIC radio is used for background scanning.
Step 4	**map-fast-ancestor-find** **Example:** `Device(config-wireless-mesh-profile)# map-fast-ancestor-find`	Configures fast ancestor find mode.

Configuring Dot11ax Rates on Mesh Backhaul Per Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.
The **All Access Points** section, which lists all the configured APs in the network, is displayed with their corresponding details.

Step 2 Click the configured mesh AP.
The **Edit AP** window is displayed.

Step 3 Choose the **Mesh** tab.

Step 4 In the **General** section, under the **Backhaul** section, the default **Backhaul Radio Type**, **Backhaul Slot ID**, and **Rate Types** field details are displayed. Note that the values for **Backhaul Radio Type** and **Backhaul Slot ID** can be changed only for a root AP.

Step 5 From the **Rate Types** drop-down list, choose the backhaul rate type.

Based on the choice, enter the details for the corresponding fields that are displayed. The backhaul interface varies between auto and 802.11a/b/g/n/ac/ax rates depending upon the AP. Cisco Catalyst 9124AX Outdoor Access Point is the only AP that support 11ax backhaul rates on the mesh backhaul.

Step 6 In the **Backhaul MCS Index** field, enter the Modulation Coding Scheme (MCS) rate, that can be transmitted between the APs. The valid range is from 0 to 11, on both the bands.

Step 7 In the **Spatial Stream** field, enter the number of spatial streams that are supported. The maximum number of spatial streams supported on a single radio in a 5-GHz radio band is 8, while 2.4-GHz radio band supports 4 spatial streams.

Step 8 Click **Update and Apply to Device**.

Configuring Dot11ax Rates on Mesh Backhaul in Mesh Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 2 Click **Add**.
The **Add Mesh Profile** window is displayed.

Step 3 In the **Add Mesh Profile** window, click the **General** tab.

Step 4 In the **Name** field, enter the mesh profile name.

Step 5 Click the **Advanced** tab.

Step 6 In the **5 GHz Band Backhaul** section and the **2.4 GHz Band Backhaul** section, choose the **dot11ax** backhaul rate type from **Rate Types** the drop-down list.

Note Cisco Catalyst 9124AXI/D Series outdoor Access Point is the only AP to support 11ax backhaul rates on the mesh backhaul.

Step 7 In the **Dot11ax MCS index** field, specify the MCS rate at which data can be transmitted between the APs. The value range is between 0 to 11, on both the radio bands.

Step 8 In the **Spatial Stream** field, enter a value. The maximum number of spatial streams supported on a single radio in a 5-GHz radio band is 8, while 2.4- GHz radio band supports 4 spatial streams.

Step 9 Click **Update and Apply to Device**.

Configuring Data Rate Per AP (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **mesh backhaul rate dot11ax mcs** *<0-11>* **ss** *<1-8>* **Example:** `Device# ap name ap1 mesh backhaul rate dot11ax 5 ss 4`	Configures mesh backhaul 11ax rates for 2.4-GHz and 5-GHz bands.

Configuring Data Rate Using Mesh Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.

Step 3	**backhaul rate dot11** {**24ghz** | **5ghz**}**dot11ax mcs** *<0-11>* **spatial-stream** *<1-8>*
	Example:
	`Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11ax mcs 5 spatial-stream 6`
	`Device(config-wireless-mesh-profile)# backhaul rate dot11 24ghz dot11ax mcs 5 spatial-stream 4`
		Configures backhaul transmission rate for 2.4-GHz band and 5-GHz band. The 802.11ax spatial stream value for 2.4-GHz band is from 1 to 4, and the spatial stream value for the 5-GHz band is from 1to 8.

Specifying the Backhaul Slot for the Root AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Click **Add**.

Step 3 In **General** tab, enter the **Name** of the mesh profile.

Step 4 In **Advanced** tab, choose the rate types from the **Rate Types** drop-down list for **5 GHz Band Backhaul** and **2.4 GHz Band Backhaul**.

Step 5 Click **Apply to Device**.

Specifying the Backhaul Slot for the Root AP (CLI)

Follow the procedure given below to set the mesh backhaul rate.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *rap-name* **mesh backhaul radio dot11**{**24ghz** | **5ghz**} [**slot** *slot-id*] **Example:** `Device# ap name rap1 mesh backhaul radio dot11 24ghz slot 2`	Sets the mesh backhaul radio slot.

Configuring Wireless Backhaul Data Rate (CLI)

Backhaul is used to create a wireless connection between APs. A backhaul interface can be 802.11bg/a/n/ac depending on the AP. The rate selection provides for effective use of the available RF spectrum. Data rates can also affect the RF coverage and network performance. Lower data rates, for example, 6 Mbps, can extend farther from the AP than can have higher data rates, for example, 1300 Mbps. As a result, the data rate affects cell coverage, and consequently, the number of APs required.

Note You can configure backhaul data rate, preferably, through the mesh profile. In certain cases, where a specific data rate is needed, use the command to configure the data rate per AP.

Follow the procedure given below to configure wireless backhaul data rate in privileged EXEC mode or in mesh profile configuration mode.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **mesh backhaul rate** {**auto** | **dot11abg** | **dot11ac** |**dot11n**} **Example:** `Device# #ap name ap1 mesh backhaul rate auto`	Configures backhaul transmission rate.
Step 3	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 4	**backhaul rate dot11** {**24ghz** | **5ghz**}**dot11n RATE_6M** **Example:** `Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11n mcs 31`	Configures backhaul transmission rate. **Note** Note that the rate configured on the AP (step 2) should match with the rate configured on the mesh profile (step4).

Using a Link Test on Mesh Backhaul (GUI)

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **AP Statistics** > **General**.

Step 2 Click the Access Point.

Step 3 Choose **Mesh** > **Neighbor** > **Linktest**.

Step 4 Choose the desired values from the **Date Rates**, **Packets to be sent (per second)**, **Packet Size (bytes)** and **Test Duration (seconds)** drop-down lists..

Step 5 Click **Start**.

Using a Link Test on Mesh Backhaul

Follow the procedure given below to trigger linktest between neighbor mesh APs.

Note Use the **test mesh linktest mac-address** *neighbor-ap-mac* **rate** *data-rate* **fps** *frames-per-second* **frame-size** *frame-size* command to perform link test from an AP.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **mesh linktest** *dest-ap-mac data-rate packet-per-sec packet-size test-duration* **Example:** `Device# #ap name ap1 mesh linktest F866.F267.7DFB 24 234 1200 200`	Sets link test parameters.

Mesh CAC

The Call Admission Control (CAC) enables a mesh access point to maintain controlled quality of service (QoS) on the controller to manage voice quality on the mesh network. Bandwidth-based, or static CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call. Each access point determines whether it is capable of accommodating a particular call by looking at the bandwidth available and compares it against the bandwidth required for the call. If there is not enough bandwidth available to maintain the maximum allowed number of calls with acceptable quality, the mesh access point rejects the call.

- When client roams from one MAP to another in same site, bandwidth availability is checked again in the new tree for the active calls.
- When MAP roams to new parent, the active calls are not terminated and it continues to be active with other active calls in the sub tree.
- High Availability (HA) for MAPs is not supported; calls attached to MAP's access radio are terminated on HA switchover.
- HA for RAP is supported, hence calls attached to RAP's access radio continues to be active in new controller after switchover.
- Mesh CAC algorithm is applicable only for voice calls.
- For Mesh backhaul radio bandwidth calculation, static CAC is applied. Load-based CAC is not used as the APs do not support load-based CAC in Mesh backhaul.
- Calls are allowed based on available bandwidth on a radio. Airtime Fairness (ATF) is not accounted for call admission and the calls that fall under ATF policy are given bandwidth as per ATF weight.

Mesh CAC is not supported for the following scenarios.

- APs in a Mesh tree assigned with different site tags.
- APs in a Mesh tree assigned with the default site tag.

Configuring Mesh CAC (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh cac** **Example:** `Device(config)# wireless mesh cac`	Enables mesh CAC mode.

Speeding up Mesh Network Recovery Through Fast Detection of Uplink Gateway Reachability Failure

In all 802.11ac Wave 2 APs, the speed of mesh network recovery mechanism is increased through fast detection of uplink gateway reachability failure. The uplink gateway reachability of the mesh APs is checked using ICMP ping to the default gateway, either IPv4 or IPv6.

Mesh AP triggers the reachability check in the following two scenarios:

- After a new uplink is selected, until the mesh AP joins the controller

  After a new uplink is selected, the mesh AP has a window of 45 seconds to reach gateway (via static IP or DHCP) through the selected uplink. If the mesh AP still fails to reach the gateway after 45 seconds, the current uplink is in blocked list and the uplink selection process is restarted. If the AP joins the controller within this 45-second window, the reachability check is stopped. Subsequently, there is no gateway reachability check during normal operations.

- As soon as the mesh AP times out its connection with the controller

  After the mesh AP times out its connection with the controller and the AP fails to reach the gateway in 5 seconds, the current uplink is immediately added to the blocked list and the uplink selection process is restarted.

Fast Teardown for a Mesh Deployment

In mesh deployments, sometimes a root access point connects to the controller through a nonreliable link such as a wireless microwave link. If a data uplink failure occurs, client loses connectivity to detect the cause of the failure. The feature allows you to detect the root access point uplink failure faster in a mesh deployment and address fast teardown of the mesh network when uplink failure occurs on the root access point.

Note Fast Teardown for Mesh APs is not supported on Cisco Industrial Wireless (IW) 3702 Access Points.

Enabling Wireless Mesh Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**fast-teardown** **Example:** `Device(config-wireless-profile-mesh)# fast-teardown`	Enables the fast teardown of mesh network and configures the feature's parameter.

Associating Wireless Mesh to an AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile default-ap-profile`	Configures the AP profile and enters AP profile configuration mode.
Step 3	**mesh-profile** *mesh-profile-name* **Example:** `Device(config-ap-profile)# mesh-profile test1`	Configures the mesh profile in AP profile configuration mode.

Configuring Fast Teardown for a Mesh AP Profile (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Mesh > Profiles**.

Step 2 Click **Add**.

Step 3 In the **Add Mesh Profile** window, click **Advanced**.

Step 4 Select a security mode, authentication method, and authorization method.

Step 5 Enable **Ethernet bridging**, if required.

Step 6 Enter the bridge group name and enable Strict Match BGN.

Step 7 Select a band backhaul transmission rate for your radio.

Step 8 Preform the following action in the **Fast Roaming** section:

- Check the **Fast Teardown** check box to detect the root access point uplink failure faster in a mesh deployment and to address fast teardown of the mesh network when an uplink failure occurs.
- In the **Number of Retries** field, enter the number of retries allowed until gateway is considered unreachable. The valid range is between 1 to 10.
- In the **Interval value** field, enter the retry value. The valid range is between 1 to 10 seconds.
- In the **Latency Threshold** field, enter the threshold for a round-trip latency between the AP and the controller. The valid range is between 1 and 500 milliseconds.
- In the **Latency Exceeded Threshold**field, enter the latency interval in which at least one ping must succeed in less than the specified time. The valid range is between 1 to 30 seconds.
- In the **Uplink Recovery Interval** field, enter the time during which root access point uplink must be stable in order to accept the child connections. The valid range is between 1 and 3600 seconds.

Step 9 Click **Apply to Device**.

Configuring Fast Teardown for a Mesh AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters the mesh profile configuration mode.

	Command or Action	Purpose
Step 3	**fast-teardown** **Example:** `Device(config-wireless-mesh-profile)# fast-teardown`	Enables the fast teardown of mesh network and configures the feature's parameter.
Step 4	**enabled** **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# enabled`	Enables the fast teardown feature.
Step 5	**interval** *duration* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# interval 5`	(Optional) Configures the retry interval. The valid values range between 1 and 10 seconds.
Step 6	**latency-exceeded-threshold** *duration* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# latency-exceeded-threshold 20`	(Optional) Specifies the latency interval at which at least one ping must succeed in less than threshold time. The valid values range between 1 and 30 seconds.
Step 7	**latency-threshold** *threshold range* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# latency-threshold 20`	(Optional) Speficies the latency threshold. The valid values range between 1 and 500 milliseconds.
Step 8	**retries** *retry limit* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# retries 1`	(Optional) Specifies the number of retries until the gateway is considered unreachable. The valid values range between 1 and 10.
Step 9	**uplink-recovery-intervals** *recovery interval* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# uplink-recovery-intervals 1`	(Optional) Specifies the time during which root access point uplink has to be stable to accept child connections. The valid values range between 1 and 3600 seconds.

Verifying Fast Teardown with Default Mesh Profile

To verify the fast teardown with the default-mesh-profile, use the following command:

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name            default-mesh-profile
------------------------------------------------
Fast Teardown                        : ENABLED
Number of Retries                    : 4
Interval in sec                      : 1
Latency Threshold in msec            : 10
Latency Exceeded Threshold in sec    : 8
Uplink Recovery Interval in sec      : 60
```

Configuring Subset Channel Synchronization

All the channels used by all the RAPs in a controller are sent to all the MAPs for future seek and convergence. The controller keeps a list of the subset channels for each Bridge Group Name (BGN). The list of subset channels are also shared across all the controllers in a mobility group.

Subset channel list is list of channels where RAP of particular BGN are operating. This list is communicated to all the MAPs within and across the controllers. The idea of subset channel list is for faster convergence of the Mesh APs. Convergence method can be selected in mesh profile. If the convergence method is not standard then subset channel list is pushed to MAPs.

Follow the procedure given below to configure subset channel synchronization for mobility group.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh subset-channel-sync mac** **Example:** `Device(config)# wireless mesh subset-channel-sync`	Configures subset channel synchronization for a mobility group.

Selecting a Preferred Parent (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the Access Point.

Step 3 In the **Mesh** tab, enter the **Preferred Parent MAC**.

Step 4 Click **Update & Apply to Device**.

Selecting a Preferred Parent (CLI)

Follow the procedure given below to configure a preferred parent for a MAP.

Using this mechanism, you can override the AWPP-defined parent selection mechanism and force a mesh AP to go to a preferred parent.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.

Step 2	**ap name** *ap-name* **mesh parent preferred** *mac-address*
	Example:
	`Device# ap name ap1 mesh parent preferred 00:0d:ed:dd:25:8F`
		Configures mesh parameters for the AP and sets the mesh-preferred parent MAC address.
		Note Ensure that you use the radio MAC address of the preferred parent.
		For Cisco Wave 1 APs, when you configure a preferred parent, ensure that you specify the MAC address of the actual mesh neighbor for the desired parent. This MAC address is the base radio MAC address that has the letter "f" as the final character. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:0f as the preferred parent.
		`Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:0f`
		For Cisco Wave 2 APs, when you configure a preferred parent, the MAC address is the base radio MAC address that has "0x11" added to the last two characters. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:11 as the preferred parent.
		`Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:11`

Changing the Role of an AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.
Step 2 Click the **Access Point**.
Step 3 In the **Mesh** tab, choose **Root** or **Mesh** from the **Role** drop-down list.
Step 4 Click **Update & Apply to Device**.

After the role change is triggered, the AP reboots.

Changing the Role of an AP (CLI)

Follow the procedure to change the AP from MAP to RAP or vice-versa.

By default, APs join the controller in a mesh AP role.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **role** {**mesh-ap** | **root-ap**} **Example:** `Device# #ap name ap1 root-ap`	Changes the role for the Cisco bridge mode APs. After the role change is triggered, the AP reboots.

Configuring Battery State for Mesh AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**
Step 2 Choose a profile.
Step 3 In **General** tab, check the **Battery State for an AP** check box.
Step 4 Click **Update & Apply to Device**.

Configuring Battery State for Mesh AP

Some Cisco outdoor APs come with the option of battery backup. There is also a POE-out port that can power a video surveillance camera. The integrated battery can be used for temporary backup power during external power interruptions.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**battery-state** **Example:** `Device(config-wireless-mesh-profile)# battery-state`	Configures the battery state for an AP.

Verifying Mesh Configuration in Embedded Wireless Controller

Verifying Mesh Configuration

Use the following **show** commands to verify the various aspects of mesh configuration.

- **show wireless mesh stats** *ap-name*
- **show wireless mesh security-stats** {*all* | *ap-name*}
- **show wireless mesh queue-stats** {*all* | *ap-name*}
- **show wireless mesh per-stats summary** {*all* | *ap-name*}
- **show wireless mesh neighbor summary** {*all* | *ap-name*}
- **show wireless mesh neighbor detail** *ap-name*
- **show wireless mesh ap summary**
- **show wireless mesh ap tree**
- **show wireless mesh ap backhaul**
- **show wireless mesh config**

- **show wireless mesh convergence detail** *bridge-group-name*
- **show wireless mesh convergence subset-channels**
- **show wireless mesh neighbor**
- **show wireless profile mesh detailed** *mesh-profile-name*
- **show wireless stats mesh security**
- **show wireless stats mesh queue**
- **show wireless stats mesh packet error**
- **show wireless mesh ap summary**
- **show ap name** *ap-name* **mesh backhaul**
- **show ap name** *ap-name* **mesh neighbor detail**
- **show ap name** *ap-name* **mesh path**
- **show ap name** *ap-name* **mesh stats packet error**
- **show ap name** *ap-name* **mesh stats queue**
- **show ap name** *ap-name* **mesh stats security**
- **show ap name** *ap-name* **mesh stats**
- **show ap name** *ap-name* **mesh bhrate**
- **show ap name** *ap-name* **config ethernet**
- **show ap name** *ap-name* **cablemodem**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **gps location**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **mesh linktest data** *dest-mac*
- **show ap environment**
- **show ap gps location**

For details about these commands, see the Cisco Catalyst 9800 Series Wireless Controller Command Reference document.

MAC Authorization

Use the following **show** command to verify the MAC authorization configuration:

```
Device# show run aaa
aaa authentication dot1x CENTRAL_LOCAL local
aaa authorization credential-download CENTRAL_AUTHOR local
username 002cc8de4f31 mac
username 00425a0a53b1 mac

ewlc_eft#sh wireless profile mesh detailed madhu-mesh-profile
```

```
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abbc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
...
Battery State                 : ENABLED
Authorization Method          : CENTRAL_AUTHOR
Authentication Method         : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

PSK Provisioning

Use the following **show** command to verify PSK provisioning configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                 :  4
  Recommended Max Children for MAP              : 10
  Recommended Max Children for RAP              : 20
  Low Link SNR                                  : 12
  High Link SNR                                 : 60
  Max Association Number                        : 10
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
  PSK In-use key number                         : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

Bridge Group Name

Use the following **show** command to verify the bridge group name configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
```

```
Multicast Mode                : In-Out
Range in feet                 : 12000
Security Mode                 : EAP
Convergence Method            : Fast
LSC only Authentication       : DISABLED
Battery State                 : ENABLED
Authorization Method          : CENTRAL_AUTHOR
Authentication Method         : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

Backhaul Client Access

Use the following **show** command to verify the backhaul client access configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
...
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

Wireless Backhaul Data Rate

Use the following **show** command to verify the wireless backhaul data rate configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
...
Authorization Method          : CENTRAL_AUTHOR
Authentication Method         : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

Dynamic Frequency Selection

Use the following **show** command to verify the dynamic frequency selection configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
```

```
Full Sector DFS                : ENABLED
...
Backhaul tx rate(802.11a)      : 802.11n mcs15
```

Intrusion Detection System

Use the following **show** command to verify the wireless backhaul data rate configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name              : abc-mesh-profile
-------------------------------------------------
Description                    :
Bridge Group Name              : bgn-abc
Strict match BGN               : ENABLED
Amsdu                          : ENABLED
Background Scan                : ENABLED
Channel Change Notification    : DISABLED
Backhaul client access         : ENABLED
Ethernet Bridging              : ENABLED
Ethernet Vlan Transparent      : DISABLED
Full Sector DFS                : ENABLED
IDS                            : ENABLED
Multicast Mode                 : In-Out
...
Backhaul tx rate(802.11a)      : 802.11n mcs15
```

Ethernet Bridging

Use the following **show** command to verify ethernet bridging configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name              : abc-mesh-profile
-------------------------------------------------
Description                    :
Bridge Group Name              : bgn-abc
Strict match BGN               : ENABLED
Amsdu                          : ENABLED
Background Scan                : ENABLED
Channel Change Notification    : DISABLED
Backhaul client access         : ENABLED
Ethernet Bridging              : ENABLED
Ethernet Vlan Transparent      : DISABLED
Full Sector DFS                : ENABLED
IDS                            : ENABLED
Multicast Mode                 : In-Out
...
Backhaul tx rate(802.11a)      : 802.11n mcs15
```

Multicast over Mesh

Use the following **show** command to verify multicast over Mesh configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name              : abc-mesh-profile
-------------------------------------------------
Description                    :
Bridge Group Name              : bgn-abc
Strict match BGN               : ENABLED
Amsdu                          : ENABLED
Background Scan                : ENABLED
Channel Change Notification    : DISABLED
Backhaul client access         : ENABLED
Ethernet Bridging              : ENABLED
```

```
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
Multicast Mode                : In-Out
...
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

RRM on Mesh Backhaul

Use the following **show** command to verify RRM on Mesh backhaul configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                    : ENABLED
  Mesh CAC                                        : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)     : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed         : ENABLED
  Rap Channel Sync                                : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                   :  4
  Recommended Max Children for MAP                : 10
  Recommended Max Children for RAP                : 20
  Low Link SNR                                    : 12
  High Link SNR                                   : 60
  Max Association Number                          : 10
  Parent Change Number                            :  3

Mesh PSK Config
  PSK Provisioning                                : ENABLED
  Default PSK                                     : ENABLED
  PSK In-use key number                           : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

Preferred Parent Selection

Use the following **show** command to verify preferred parent configuration:

```
Device# show wireless mesh ap tree
=========================================================================
AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
=========================================================================

[Sector 1]
-----------
1542-RAP [0, 0, bgn-madhu, (165), 0000.0000.0000, 1%, 0]
   |-MAP-2700 [1, 67, bgn-madhu, (165), 7070.8b7a.6fb8, 0%, 0]

Number of Bridge APs : 2
Number of RAPs : 1
Number of MAPs : 1

(*)  Wait for 3 minutes to update or Ethernet Connected Mesh AP.
(**) Not in this Controller
```

AP Role Change

Use the following **show** command to verify AP role change configuration:

```
Device# show wireless mesh ap summary
AP Name                          AP Model BVI MAC        BGN        AP Role
-------                          -------- -------        ---        -------
1542-RAP                         1542D    002c.c8de.1338 bgn-abc  Root AP
MAP-2700                         2702I    500f.8095.01e4 bgn-abc  Mesh AP

Number of Bridge APs         :   2
Number of RAPs               :   1
Number of MAPs               :   1
Number of Flex+Bridge APs    :   0
Number of Flex+Bridge RAPs   :   0
Number of Flex+Bridge MAPs   :   0
```

Mesh Leaf Node

Use the following **show** command to verify mesh leaf node configuration:

```
Device# show ap name MAP-2700 config general
Cisco AP Name   : MAP-2700
================================================

Cisco AP Identifier                              : 7070.8bbc.d3e0
Country Code                                     : Multiple Countries : IN,US,IO,J4
Regulatory Domain Allowed by Country             : 802.11bg:-AEJPQU   802.11a:-ABDJNPQU
AP Country Code                                  : IN  - India
AP Regulatory Domain
  Slot 0                                         : -A
  Slot 1                                         : -D
MAC Address                                      : 500f.8095.01e4
...
AP Mode                                          : Bridge
Mesh profile name                                : abc-mesh-profile
AP Role                                          : Mesh AP
Backhaul radio type                              : 802.11a
Backhaul slot id                                 : 1
Backhaul tx rate                                 : auto
Ethernet Bridging                                : Enabled
Daisy Chaining                                   : Disabled
Strict Daisy Rap                                 : Disabled
Bridge Group Name                                : bgn-abc
Strict-Matching BGN                              : Enabled
Preferred Parent Address                         : 7070.8b7a.6fb8
Block child state                                : Disabled
PSK Key Timestamp                                : Not Configured
...
FIPS status                                      : Disabled
WLANCC status                                    : Disabled
GAS rate limit Admin status                      : Disabled
WPA3 Capability                                  : Disabled
EWC-AP Capability                                 : Disabled
AWIPS Capability                                 : Disabled
Proxy Hostname                                   : Not Configured
Proxy Port                                       : Not Configured
Proxy NO_PROXY list                              : Not Configured
GRPC server status                               : Disabled
```

Subset Channel Synchronization

Use the following **show** command to verify the subset channel synchronization configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                   : ENABLED
```

```
  Mesh CAC                                        : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)     : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed         : ENABLED
  Rap Channel Sync                                : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                   :  4
  Recommended Max Children for MAP                : 10
  Recommended Max Children for RAP                : 20
  Low Link SNR                                    : 12
  High Link SNR                                   : 60
  Max Association Number                          : 10
  Parent Change Number                            :  3

Mesh PSK Config
  PSK Provisioning                                : ENABLED
  Default PSK                                     : ENABLED
  PSK In-use key number                           : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

Provisioning LSC for Bridge-Mode and Mesh APs

Use the following **show** command to verify the provisioning LSC for Bridge-Mode and Mesh AP configuration:

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name             : default-mesh-profile
-------------------------------------------------
Description                   : default mesh profile
Bridge Group Name             : bgn-abc
Strict match BGN              : DISABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : ENABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : DISABLED
Ethernet Vlan Transparent     : ENABLED
Full Sector DFS               : ENABLED
IDS                           : DISABLED
Multicast Mode                : In-Out
Range in feet                 : 12000
Security Mode                 : EAP
Convergence Method            : Fast
LSC only Authentication       : DISABLED
Battery State                 : ENABLED
Authorization Method          : default
Authentication Method         : default
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : auto
```

Specify the Backhaul Slot for the Root AP

Use the following **show** command to verify the backhaul slot for the Root AP configuration:

```
Device# show ap name 1542-RAP mesh backhaul
MAC Address : 380e.4d85.5e60
  Current Backhaul Slot: 1
  Radio Type: 0
  Radio Subband: All
  Mesh Radio Role: DOWNLINK
```

```
  Administrative State: Enabled
  Operation State: Up
  Current Tx Power Level:
  Current Channel: (165)
  Antenna Type: N/A
  Internal Antenna Gain (in .5 dBm units): 18
```

Using a Link Test on Mesh Backhaul

Use the following **show** command to verify the use of link test on mesh backhaul configuration:

```
Device# show ap name 1542-RAP mesh linktest data 7070.8bbc.d3ef
380e.4d85.5e60 ==> 7070.8bbc.d3ef

Started at : 05/11/2020 20:56:28
Status: In progress

Configuration:
==============
Data rate:  Mbps
Packets per sec: : 234
Packet Size: : 1200
Duration: : 200
```

Mesh CAC

Use the following **show** command to verify mesh CAC configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                 :  4
  Recommended Max Children for MAP              : 10
  Recommended Max Children for RAP              : 20
  Low Link SNR                                  : 12
  High Link SNR                                 : 60
  Max Association Number                        : 10
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
  PSK In-use key number                         : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

Verifying Mesh Convergence

The following is a sample output of the **show wireless profile mesh detailed** command that displays the mesh convergence method used:

```
Device# show wireless profile mesh detailed default-mesh-profile
```

```
Mesh Profile Name             : default-mesh-profile
------------------------------------------------
Description                 : default mesh profile
Convergence Method          : Fast
```

The following is a sample output of the **show wireless mesh convergence subset-channels** command that displays the subset channels of the selected bridge group name:

```
Device# show wireless mesh convergence subset-channels

Bridge group name                Channel
----------------------------------------
Default                          132
```

Verifying Mesh Backhaul

The following is a sample output of the **show ap name mesh backhaul** command that shows details of the mesh backhaul at 2.4 GHz:

```
Device# show ap name test-ap mesh backhaul

MAC Address : xxxx.xxxx.xxxx
Current Backhaul Slot: 0
Radio Type: 0
Radio Subband: All
Mesh Radio Role: DOWNLINK
Administrative State: Enabled
Operation State: Up
Current Tx Power Level:
Current Channel: (11)
Antenna Type: N/A
Internal Antenna Gain (in .5 dBm units): 0
```

The following is a sample output of the **show wireless mesh ap backhaul** command that shows the mesh backhaul details:

```
Device# show wireless mesh ap backhaul

MAC Address : xxxx.xxxx.0x11
Current Backhaul Slot: 1
Radio Type: Main
Radio Subband: All
Mesh Radio Role: Downlink
Administrative State: Enabled
Operation State: Up
Current Tx Power Level: 6
Current Channel: (100)*
Antenna Type: N/A
Internal Antenna Gain (in .5 dBm units): 10
```

The following is a sample output of the **show ap summary** command that shows the radio MAC address and the corresponding AP name:

```
Device# show ap summary
Number of APs: 1
AP Name    Slots  AP Model         Ethernet       MAC Radio MAC  Location         Country
IP Address   State
-----------------------------------------------------------------------------------------------------------------
AP-Cisco-1  2     AIR-APXXXXX-E-K9 xxxx.xxxx.xxd4 xxxx.xxxx.0x11 default location  DE
10.11.70.170 Registered
```

Verifying Mesh Ethernet Daisy Chaining

- The following is a sample output of the **show ap config general** command that displays whether a persistent SSID is configured for an AP.

```
Device# show ap 3702-RAP config general

Persistent SSID Broadcast                  Enabled/Disabled
```

- The following is a sample output of the **show wireless mesh persistent-ssid-broadcast summary** command that displays the persistent SSID broadcast status of all the bridge RAPs.

```
Device# show wireless mesh persistent-ssid-broadcast summary

 AP Name     AP Model BVI MAC        BGN        AP Role               Persistent SSID
state
-------     -------- -------       ---       -------             ----------------------
3702-RAP     3702     5c71.0d07.db50 ap_name    Root AP              Enabled
1560-RAP    1562E    380e.4dbf.c6b0 ap_name    Root AP             Disabled
```

Verifying Dot11ax Rates on Mesh Backhaul

To verify the 802.11ax rates on mesh backhaul in the mesh profile, use the following command:

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name             : default-mesh-profile
-------------------------------------------------
Description                   : default mesh profile
.
.
Backhaul tx rate(802.11bg)    : 802.11ax mcs7 ss1
Backhaul tx rate(802.11a)     : 802.11ax mcs9 ss2
```

To verify the 802.11ax rates on mesh backhaul in the general configuration of an AP, use the following command:

```
Device# show ap config general
Cisco AP Identifier            : 5c71.0d17.49e0
.
.
Backhaul slot id               : 1
Backhaul tx rate               : 802.11ax mcs7 ss1
```

Verifying Background Scanning and MAP Fast Ancestor Find

To verify if the Background Scanning and MAP Fast Ancestor Find features are enabled, run the **show wireless profile mesh detailed** command:

```
Device# show wireless profile mesh detailed Mesh_Profile | i Background Scan
Background Scan               : ENABLED

Device# show wireless profile mesh detailed Mesh_Profile | i MAP fast ancestor find
MAP fast ancestor find        : ENABLED
```