Mesh Access Points

- Mesh network, on page 3
- Restrictions for Mesh Access Points, on page 5
- MAC authorization, on page 5
- Preshared key provisioning, on page 6
- EAP authentication, on page 6
- Bridge group names, on page 7
- Mesh background scanning, on page 8
- Mesh backhaul at 2.4 GHz and 5 GHz , on page 9
- Mesh serial backhaul, on page 10
- Mesh backhaul RRM, on page 11
- Dynamic frequency selection, on page 12
- Country codes, on page 12
- Intrusion detection system, on page 13
- Mesh interoperability between controllers, on page 13
- DHCP and NAT functionality on root AP (RAP), on page 13
- Mesh convergence, on page 14
- Ethernet bridging, on page 15
- Multicast over mesh Ethernet bridging network, on page 16
- Radio Resource Management on mesh, on page 17
- Air Time Fairness on Mesh, on page 17
- Spectrum Intelligence for mesh, on page 18
- Indoor mesh interoperability with outdoor mesh, on page 18
- Workgroup bridge, on page 19
- Link test, on page 19
- Mesh daisy chaining, on page 20
- Mesh leaf node, on page 21
- FlexConnect + bridge mode, on page 21
- Backhaul client access, on page 22
- Mesh call admission control, on page 22
- Mesh network recovery mechanisms, on page 22
- Fast teardown for a mesh deployment, on page 23
- Configure MAC authorization (GUI), on page 23
- Configure MAC authorization (CLI), on page 24

- Configure MAP authorization - EAP (GUI), on page 25
- Configure MAP authorization (CLI), on page 26
- Configure PSK provisioning (CLI), on page 27
- Configure a bridge group name (GUI), on page 28
- Configure a bridge group name (CLI), on page 28
- Configure background scanning (GUI), on page 29
- Configure background scanning, on page 30
- Configure AP fast ancestor find mode (GUI), on page 30
- Configure background scanning and MAP fast ancestor find mode (Task), on page 31
- Configure backhaul client access (GUI), on page 32
- Configure backhaul client access (CLI), on page 32
- Configure dot11ax rates on mesh backhaul per AP (GUI), on page 33
- Configuring Dot11ax Rates on Mesh Backhaul in Mesh Profile (GUI), on page 34
- Configure wireless backhaul data rate (CLI), on page 34
- Configure data rate per AP (CLI), on page 35
- Configure data rate using mesh profile (CLI), on page 36
- Configure mesh backhaul (CLI), on page 36
- Configure dynamic frequency selection (CLI), on page 37
- Configure the intrusion detection system (CLI), on page 38
- Configure Ethernet bridging (GUI), on page 38
- Configure Ethernet bridging (CLI), on page 39
- Configure multicast modes over mesh, on page 41
- Configure RRM on mesh backhaul (CLI), on page 41
- Configure RRM channel assignment for root access points globally, on page 42
- Configure RRM channel assignment for an AP, on page 43
- Select a preferred parent (GUI), on page 44
- Select a preferred parent (CLI), on page 44
- Change the role of an AP (GUI), on page 45
- Change the role of an AP (CLI), on page 45
- Configure mesh leaf node (CLI), on page 46
- Configure the mesh leaf node (GUI), on page 47
- Configure subset channel synchronization , on page 47
- Provision LSC for bridge-mode and mesh APs (GUI), on page 48
- Provision LSC for bridge-mode and mesh APs, on page 48
- Specify the backhaul slot for the root AP (GUI), on page 49
- Specify the backhaul slot for the root AP (CLI), on page 50
- Use a link test on mesh backhaul (GUI), on page 50
- Use a link test on mesh backhaul, on page 51
- Configure battery state for mesh AP (GUI), on page 52
- Configure battery state for mesh AP (CLI), on page 52
- Configure mesh convergence (CLI), on page 53
- Configure DHCP server on root AP (CLI), on page 53
- Configure mesh Ethernet daisy chaining (CLI), on page 54
- Enable mesh Ethernet daisy chaining, on page 54
- Configure mesh CAC (CLI), on page 55
- Configure ATF on mesh (GUI), on page 56

- Configure ATF on mesh, on page 56
- Create an ATF policy for a MAP, on page 57
- Create an ATF policy (GUI), on page 57
- Add an ATF to a policy profile (GUI), on page 58
- Enable ATF mode in an RF profile (GUI), on page 58
- Enable wireless mesh profile (CLI), on page 59
- Enable serial backhaul in radio profile (GUI), on page 59
- Enable mesh configurations in radio profile (CLI), on page 60
- Enable serial backhaul (CLI), on page 61
- Associate wireless mesh to an AP profile (CLI), on page 62
- Configure fast teardown for a mesh AP profile (GUI) , on page 63
- Configure fast teardown for a mesh AP profile (CLI), on page 64
- Flex Resilient with Flex and Bridge Mode Access Points, on page 65
- Verify ATF configuration on mesh, on page 72
- Verify mesh Ethernet daisy chaining, on page 73
- Verify mesh convergence, on page 73
- Verify DHCP server for root AP configuration, on page 73
- Verify mesh backhaul, on page 74
- Verify mesh configuration, on page 74
- Verify dot11ax rates on mesh backhaul, on page 83
- Verify mesh serial backhaul, on page 83
- Verify the RRM DCA status, on page 84
- Verify fast teardown with default mesh profile, on page 84
- Verify background scanning and MAP fast ancestor find, on page 84

Mesh network

A mesh network is a wireless network topology that

- uses interconnected Cisco Aironet outdoor mesh APs and indoor mesh APs to relay data
- provides scalability, central management, and seamless mobility between indoor and outdoor deployments, and
- is coordinated and provisioned using Cisco Wireless Controller and Cisco Prime Infrastructure.

The Control and Provisioning of Wireless Access Points (CAPWAP) protocol manages the connection of mesh access points to the network, ensuring secure and efficient network operations.

End-to-end security

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

Wireless mesh termination points

The wireless mesh terminates at two points on the wired network. The first location is where the root access point (RAP) is attached and all bridged traffic connects to the wired network. The second location is where

the CAPWAP controller connects to the wired network. At this location, the WLAN client traffic from the mesh network connects to the wired network. The WLAN client traffic from CAPWAP is tunneled to Layer 2. Matching WLANs should terminate on the same switch VLAN as the wireless controllers. 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.

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 exist and that the corresponding AP is added to the appropriate site-tag.

Mesh scenarios in IRCM

Important These are the mesh scenarios in IRCM from Cisco IOS XE Amsterdam 17.3 up to Cisco IOS XE Cupertino 17.9, for the Cisco Wave 1 APs that are not supported:

- Cisco Wave 1 APs are not supported in the releases after Cisco IOS XE Amsterdam 17.3. This includes mesh support as well. Therefore, it is not possible for a Cisco Wave 1 AP to join a Cisco Catalyst 9800 Series Wireless Controller (controller) with Cisco IOS XE Amsterdam 17.4 and later versions. We recommend this deployment mode for Cisco Wave 1 APs.
- In the case of Cisco mesh deployments, these are the deployment limitations to be aware of when the system is deployed:
  - MAP roaming is not allowed between Cisco Catalyst 9800 Series Wireless Controllers, if the controllers run different Cisco IOS XE versions (running on versions Cisco IOS XE Amsterdam 17.3 or Cisco IOS XE Cupertino 17.9) for any of the Cisco Wave 1 APs and Cisco Wave 2 APs.
  - You cannot have Cisco Wave 1 APs and Cisco Catalyst 9124 Series APs in the same mesh tree, in the releases post Cisco IOS XE Amsterdam 17.3.x. This can be achieved in 17.3.x, starting with the 17.3.6 (upcoming) release.
  - The whole mesh tree containing Cisco Wave 1 APs must be joined to the 17.3 controller, by running the **strict-bgn** and **mac filtering** commands.

Note The limitations mentioned above are not valid for the Cisco Industrial Wireless 3702 Se which are supported until the Cisco IOS XE Cupertino 17.9 release.

Mesh RRM feature support and evolution across AP generations

This topic describes the mesh Radio Resource Management (RRM) feature support, its evolution across different generations of Cisco APs, differences between AP families, key features, and the progression of mesh RRM capabilities in various software releases.

Mesh AP families

The two families of mesh APs available are the Cisco Wave 1 APs and the Cisco Wave 2 APs and the AX APs. These families have different capabilities and features, and they are not fully compatible with each other. The Cisco Wave 1 APs do not support the same feature set as the Cisco Wave 2 and AX APs.

Both families of APs support background scanning. However, their implementations are not interoperable, so you cannot use both in a single mesh deployment.

Evolution in the mesh RRM feature across AP generations

Cisco Wave 1 APs have not received significant mesh RRM feature updates after the Cisco IOS XE Amsterdam 17.3 release. Mesh RRM features on Cisco Wave 2 and AX APs have gained many improvements in recent releases.

- Cisco IOS XE Cupertino 17.9.1 introduced mesh RRM DCA using radio information only from RAPs.
- Cisco IOS XE Dublin 17.11 introduced mesh background scanning and FastaAncestor find mode.
- Cisco IOS XE 17.14 introduced mesh RRM DCA that uses radio information from the entire mesh tree.

Restrictions for Mesh Access Points

For information about APs that support Mesh feature, see https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html.

The following mesh features are not supported:

- Serial backhaul AP support with separate backhaul radios for uplink and downlink.
- Public Safety channels (4.9-GHz band) support.
- Passive Beaconing (Anti-Stranding)

Note

- Only Root APs support SSO. MAPs will disconnect and rejoin after SSO.

  The AP Stateful Switch Over (SSO) feature allows the access point (AP) to establish a CAPWAP tunnel with the Active controller and share a mirror copy of the AP database with the Standby controller. The overall goal for the addition of AP SSO support to the controller is to reduce major downtime in wireless networks due to failure conditions that may occur due to box failover or network failover.
- In a mixed regulatory domain mesh AP deployment, ensure that the Dynamic Channel Assignment (DCA) allowed channel list is supported by MAPs.
- When you disable the admin state on the 2.4-GHz radio of mesh APs, and the root AP (RAP) backhaul radio is switched to 2.4-GHz, RAP will still use 2.4-GHz radio to serve the mesh backhaul connections, inspite of 2.4-GHz radio being in the disabled state.

MAC authorization

A MAC authorization is a security mechanism that

- restricts MAPs from joining a controller unless their MAC address is pre-approved
- ensures only authorized mesh APs participate in the wireless network, and

- can be handled using either an internal list or an external AAA server.

You must enter the MAC address of an AP in the controller for a MAP to join the controller. The controller responds only to CAPWAP requests from MAPs listed in its authorization list. Remember to use the MAC address provided on the back of the AP.

MAC authorization for MAPs connected to the controller over Ethernet occurs during the CAPWAP join process. For MAPs joining the controller over radio, MAC authorization occurs when the corresponding AP attempts to secure an adaptive wireless path protocol (AWPP) link with the parent MAP. AWPP operates as the protocol for Cisco mesh networks.

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

Preshared key provisioning

A preshared key (PSK) is a mesh security credential that

- provides authentication between Mesh Access Points (MAPs), RAPs, and controllers
- allows for custom configuration to restrict network access, and
- enhances security compared to default or wildcard provisioning based on MAC addresses.

In mesh deployments, the MAPs might leave the network and join other mesh networks if both mesh deployments use AAA with wildcard MAC filtering to allow MAP association.

Since MAPs might use EAP-FAST, you cannot control this because EAP uses a combination of MAC address and AP type for authentication, and there are no controlled configuration options available. If you use the PSK option with a default pass phrase, you create a security risk.

This issue frequently occurs in overlapping deployments of two service providers when MAPs are used in moving vehicles, such as ferries, ships, or other public transportation.

In these scenarios, your MAPs are not restricted to your service provider mesh network. As a result, another service provider's network can hijack MAPs, preventing them from serving your customers.

The PSK key provisioning feature enables network administrators to assign unique preshared keys from the controller to MAPs. This ensures that only authorized MAPs can authenticate to specific RAPs and controllers. These measures prevent accidental or malicious association with unauthorized mesh networks and protect service provider deployments.

EAP authentication

A EAP authentication is a wireless network authentication method that

- allows users and wireless clients to be authenticated locally on a controller
- removes dependence on external authentication servers, and
- supports additional modules such as LSC-based authentication for enhanced security.

Use Local EAP in remote offices to maintain connectivity during backend disruptions. The controller acts as both a server and a user database, retrieving user credentials locally or through LDAP. Local EAP supports the EAP-FAST method for MAP authentication.

An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. The controller uses these credentials to authenticate the user.

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

Locally significant certificate-based (LSC) EAP authentication

A locally significant certificate-based authentication is a WLAN security method that

- authenticates network devices (such as APs and controllers) using locally generated digital certificates
- allows both locally significant certificates (LSCs) and manufacturing installed certificates (MICs) to coexist (with LSCs taking precedence), and
- supports advanced security features, like mesh EAP authentication and master session key generation.

LSC-based EAP authentication requires a public key infrastructure (PKI). This establishes certification authorities, defines policies, and sets validity periods and restrictions.

Certificates (LSCs) must be generated and installed on Access Points and controllers. If an Access Point is provisioned with an LSC, the MIC certificate is not used during boot-up. Changes from LSC to MIC require the Access Point to reboot. LSC-based EAP authentication is supported for mesh Access Points (MAPs). The controller supports mesh security with EAP authentication to a designated server to authenticate mesh child Access Points and generate master session keys for packet encryption.

If a customer installs an LSC (certificate they generate), the AP will use that certificate for authentication and not the factory-installed MIC. Mesh child APs can use LSC EAP authentication to securely join the network and establish encrypted sessions.

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

A bridge group name (BGN) is a mesh network configuration parameter that

- controls the association of Mesh Access Points (MAPs) to a parent mesh AP
- allows logical grouping of radios to isolate different networks on the same channel, and
- allows MAPs to join networks before you assign a custom BGN.

BGNs can logically group radios to avoid two networks on the same channel from communicating with each other. The setting is useful when your network contains multiple RAPs in the same sector (area). A BGN is a string containing up to 10 characters.

A BGN of *NULL VALUE* is assigned by default during manufacturing. This value is not visible to you, but it allows a MAP to join the network before you assign a network-specific BGN.

If you have two RAPs in your network in the same sector, we recommend that you configure the two RAPs with the same BGN, on different channels.

When Strict Match BGN is enabled on a MAP, the MAP scans ten times to find a matching BGN parent. If the AP does not find a parent with a matching BGN after ten scans, it connects to a nonmatching BGN and maintains the connection for 15 minutes. After 15 minutes, the AP scans ten times again, and this cycle continues. The default BGN functionality does not change when Strict Match BGN is enabled.

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

Preferred parent selection

A preferred parent selection is a mesh network configuration method that

- enables enforcement of linear topology in a mesh environment
- allows administrators to override the AWPP-defined (Adaptive Wireless Path Protocol) parent selection algorithm, and
- supports explicit specification of the uplink path for the MAP in mesh deployments.

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
```

Mesh background scanning

A mesh background scan is a mesh networking feature that

- enables mesh access points (MAPs) to find and connect to better potential parents across channels
- maintains stable uplinks by proactively scanning for available parent nodes, and
- reduces reconnection delay after parent loss by using a neighbor list instead of scanning all channels.

When background scanning is disabled, a MAP has to scan all the channels of the regulatory domain after detecting a parent loss in order to find a new parent and go through the authentication process. This delays the time taken for the mesh AP to connect back to the controller.

When background scanning is enabled, a MAP can avoid scanning across the channels to find a parent after detecting a parent loss, and select a parent from the neighbor list and establish the Adaptive Wireless Path Protocol (AWPP) link.

Background scanning and MAP fast ancestor find mode

Cisco mesh access points (MAPs) perform the following functions:

- Interconnects over wireless links in a tree topology,
- Uses Adaptive Wireless Path Protocol (AWPP) to create and maintain their topology, and
- Supports additional features: Background Scanning and MAP Fast Ancestor Finding.

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.

Background scanning and MAP Fast Ancestor Finding feature

The Background scanning feature:

- Updates MAPs about neighboring channels and helps find new parents swiftly by scanning all available channels.
- Minimizes the time spent during scan-and-seek phases when a MAP loses its current parent.
- Does not speed up the authentication process to the new parent.

A child MAP maintains its uplink with its parent by using the AWPP adjacency request/response messages, which act as keepalive signals. If consecutive response messages are lost, the parent is considered lost, and the child MAP searches for a new parent. A MAP maintains a list of neighbors on the current ON channel. If 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 process is time-consuming.

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

Mesh backhaul at 2.4 GHz and 5 GHz

A backhaul is a wireless network interface that

- creates the connection between Mesh Access Points (MAPs)
- operates over 802.11a/n/ac/g, depending on the AP, and
- typically defaults to the 5-GHz frequency band.

Selecting the appropriate backhaul rate is important for efficient spectrum use. It can directly affect client device throughput, a critical metric in evaluating wireless performance.

Mesh backhaul is supported at 2.4 GHz and 5 GHz. By default, the backhaul interface for mesh APs uses 802.11a/ac/ax. In some countries, mesh networks cannot use a 5 GHz backhaul. In countries where 5 GHz is allowed, using 2.4 GHz radio frequencies achieves more extensive mesh or bridge distances.

When a RAP receives a slot-change configuration, the RAP propagates it to all child MAPs. All MAPs disconnect and join the newly configured backhaul slot.

For information about APs that support mesh backhaul, see https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html .

Note In Israel, you must ensure that you run the **ap country IO** command to enable the outdoor country code for the selected radio. After you configure using the **ap country IO** command, the 2.4-GHz radio is enabled and 5-GHz radio is disabled.

Mesh serial backhaul

A mesh serial backhaul is a wireless mesh networking feature that

- enables separate uplink and downlink channels on dedicated radios to improve backhaul bandwidth
- allows inbound and outbound traffic to use exclusive communication paths for better performance (one radio is used as the uplink radio and a different one is used as the downlink radio), and
- supports universal access by extending network reach and avoiding shared-channel interference.

The Mesh Serial Backhaul feature is supported in the controller from Cisco IOS XE Cupertino 17.7.1 onwards for Cisco Catalyst 9124AXE outdoor APs. To enable this feature, associate a radio profile with a radio frequency (RF) tag. When you enable this feature, all APs with the same mesh profile share the mesh configuration. All APs with the same radio profile share the radio configuration.

The 2.4-GHz and 5-GHz radios, which are not used in serial backhaul, provide basic client access functionality. The downlink radio provides universal access.

Note Slot 1 and slot 0 are supported as mesh backhaul. Slot 2 is not supported as a mesh backhaul. You can utilize slot 2 for client serving or for serial backhaul downlink.

Channel assignment

For the Mesh Serial Backhaul feature, channels are assigned according to these rules:

- Uplink and downlink channels are different.
- All the 5-GHz radios maintain a frequency guard between their operating channels. For example, 100-MHz channel spacing between radios in Cisco Catalyst 9124AXE outdoor APs.
- Dynamic Frequency Selection (DFS) channels are supported.

In a root access point, the controller assigns channels because the uplink is wired. A mesh access point uses the last channel configured by the controller for this radio or uses the default channel. If the channel used by the MAP is not compatible with the uplink, the MAP picks a valid random channel and notifies the controller. In another scenario, when the MAP receives a channel change alert on the uplink radio, it randomly picks a new downlink channel. The MAP checks the validity of the downlink radio. If the current channel is not compatible, the MAP picks a random channel.

Prerequisites for channel assignment

Ensure that these prerequisites are met before channel assignment:

- Enable tri-radio globally by running the **Device# ap tri-radio** command.

- Enable the dual radio on the APs by running the **Device# ap name** *ap-name* **dot11 5ghz dual-radio mode enable**command.

Use cases

These are some of the use cases for the Mesh Serial Backhaul feature:

- **Maximize throughput** : Serial backhaul allows the 5-GHz backhaul to operate on different channels, thereby maximizing throughput over multiple mesh hops.
- **Network segregation**: APs that have serial backhaul enabled, segregate backhaul channel on mesh topographies. This avoids localized link interferences.

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 occurred 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.

To avoid a poor channel backhaul selection, from Cisco IOS XE Dublin 17.14.1 onwards, the RRM DCA optimizes the RAP backhaul radio channel of a mesh subtree by considering the noise, interference, load, and the RF parameter measurements only from the RAP. The RRM DCA on Mesh Backhaul feature enables DCA to make better channel assignment for a mesh subtree, by having continuous measurements and inputs from the whole mesh tree required to run DCA.

To enable RRM DCA on a full mesh tree run the **wireless mesh backhaul rrm auto-dca** command. To trigger DCA once, run the **ap dot11 [5ghz | 2.4 ghz] rrm channel-update mesh** command.

To understand what happened during a DCA run on the mesh backhaul, use the **show wireless mesh rrm dca status** and **show wireless mesh rrm dca changed** commands.

Note

- In a topology with mixed APs (RF ASIC capable and non-capable APs), only inputs from the RF ASIC capable APs apply for **auto-dca**.
- All mesh APs in a subtree should be configured to belong to the same site-tag for DCA to work properly.
- This feature is limited to RF ASIC capable APs, such as Cisco Catalyst 9124 Series APs and Cisco Catalyst 9130 Series APs.

Dynamic frequency selection

A dynamic frequency selection (DFS) is a wireless communication protocol that

- enables radio devices to detect radar signals
- requires devices to cease transmission when radar is detected, and
- requires selecting and monitoring a new channel before resuming transmission.

Regulatory bodies enforce DFS to prevent interference with radar services in shared frequency bands by unlicensed wireless devices.

To protect radar services, regulatory bodies require devices on newly opened frequency sub-bands to operate using DFS. Your radio device must detect radar signals as required. If a radar event is detected in any AP within a sector, mesh access points immediately switch channels to maintain compliance.

For instance, 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.

Country codes

A country code is a regulatory compliance setting that

- allows specification of the intended country of operation for controllers and APs
- ensures adherence to local regulations about broadcast frequencies, channels, and power levels, and
- maintains correct assignment of regulatory domains for each device.

In certain countries, there is a difference for indoor and outdoor APs in these areas:

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

Controllers and APs are designed for use in many countries with varying regulatory requirements. At the factory, the radios within the APs are assigned to a specific regulatory domain (such as -E for Europe). The

country code then enables you to specify a particular country of operation (such as FR for France or ES for Spain). Configuring a country code ensures that the broadcast frequency bands, interfaces, channels, and transmit power levels of each radio are compliant with country-specific regulations.

Intrusion detection system

Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/CIPS) is a network security solution that

- monitors network traffic and system activities for signs of suspicious behavior
- detects and classifies potential security threats such as malware or unauthorized access, and
- responds to attacks or alerts administrators to enable prevention or mitigation actions.

CIDS can block specific clients from your wireless network if it detects attacks involving them in network layers 3 to 7. This feature helps you detect, classify, and stop threats such as worms, spyware, adware, network viruses, and application abuse.

Mesh interoperability between controllers

Mesh interoperability between controllers is a wireless mesh network capability that

- enables MAPs to join an AireOS controller through a mesh network formed by APs connected to a Cisco Catalyst 9800 Series Wireless Controller
- allows MAPs to join a Cisco Catalyst 9800 Series Wireless Controller through a mesh network formed by APs connected to an AireOS controller, and
- supports MAP roaming between parent mesh APs connected to AireOS and Cisco Catalyst 9800 Series Wireless Controller using PMK cache.

Note For seamless interoperability, the AireOS controller and the Cisco Catalyst 9800 Series Wireless Controller must be in the same mobility group. Both controllers should use image versions that support Inter-Release Controller Mobility (IRCM).

DHCP and NAT functionality on root AP (RAP)

DHCP and NAT functionality is a wireless network feature that

- assigns private IPv4 addresses to client devices using DHCP
- translates these private addresses to public addresses for network access with NAT, and
- enables root APs (RAPs) to provide seamless connectivity for clients in a mesh network.

The APs associated with a mesh network can play one of the two roles:

- Root Access Point (RAP) — An AP can be a root AP for multiple mesh networks.
- Mesh Access Point (MAP) — An AP can be a mesh AP for only one mesh network at a time.

Note This feature is applicable for Cisco Aironet 1542 series outdoor APs.

How DHCP and NAT functionalities work on root AP - IPv4 scenario

In wireless mesh networking, root APs (RAPs) can be enabled to provide both DHCP (Dynamic Host Configuration Protocol) and NAT (Network Address Translation) functionalities. This feature enables the controller to send a TLV to RAP when a new RAP joins the controller.

Summary

RAPs use integrated DHCP and NAT functionalities to assign private IPv4 addresses to wireless clients and provide secure, translated access to external networks. The process orchestrates communication between the network controller, RAP, and client device.

Workflow

The workflow consists of these steps:

1. The controller sends a TLV to configure the RAP with DHCP and NAT functionalities when a RAP joins the network.
2. A client device associates to the RAP's SSID.
3. The RAP assigns a private IPv4 address to the client using its DHCP functionality.
4. The RAP applies NAT to translate the client's private address, enabling secure access to external networks.

Result

Wireless clients that connect to RAPs receive private IPv4 addresses and can securely access external networks using DHCP and NAT services managed by the RAP.

Mesh convergence

A mesh convergence event is a network recovery mechanism that

- allows MAPs to re-establish connection with a controller after losing the backhaul link to the current parent
- enables the use of a maintained subset of channels for future scanning and parent identification, and
- supports multiple convergence methods to optimize reconnection time.

The table presents the supported convergence methods.

Table 1: Mesh convergence

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

Noise-tolerant fast detection

A noise-tolerant fast detection is a detection method that

- monitors the response to Adaptive Wireless Path Protocol (AWPP) neighbor requests at specified intervals
- identifies parent connectivity loss through missed responses, and
- initiates network recovery actions such as roaming or full scans when loss is detected.

Noise-tolerant fast detection occurs when there is no response to an AWPP neighbor request. In the standard method, the system evaluates the current parent every 21 seconds. Each neighbor receives a unicast request every three seconds, and the parent also receives a request. If the parent does not respond, the device either roams to an available neighbor on the same channel or performs a full scan to find a new parent.

Ethernet bridging

An Ethernet bridge is a network device that

- enables you to secure activation of Ethernet ports on MAPs
- supports both tagged and untagged packets for flexible deployment, and
- allows segmenting application traffic with VLAN tagging between wireless and wired LANs.

For security, the Ethernet port on all MAPs is disabled by default. They can be enabled only through Ethernet bridging configuration on both the root and respective MAP.

Secondary Ethernet interfaces support both tagged and untagged packets.

In a point-to-point bridging, a Cisco Aironet 1500 Series MAP can extend remote networks 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.

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.

In a mesh environment, with VLAN support for Ethernet bridging, the secondary Ethernet interfaces on MAPs are assigned a VLAN individually from the controller. Wired and wireless backhaul links operate as trunks with all VLANs allowed. 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.

Note Ensure Ethernet bridging is enabled for every parent mesh AP along the data path to the controller.

Ethernet bridging should be enabled for these scenarios:

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

VLAN tagging for MAP Ethernet clients

Primary interfaces refer to mesh AP backhauls, and secondary interfaces refer to other AP interfaces.

Ethernet VLAN tagging segments application traffic within a mesh and forwards it to a wired LAN (access mode) or another wireless mesh network (trunk mode).

Multicast over mesh Ethernet bridging network

A mesh multicast mode is a traffic management setting for bridging-enabled APs that

- determine how multicast and broadcast packets are forwarded across the mesh Ethernet network
- manage only non-CAPWAP multicast traffic, and
- help optimize bandwidth by reducing unnecessary multicast transmissions.

Mesh multicast modes

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.

Three different mesh multicast modes are available to manage multicast and broadcast packets on all MAPs. Enabling these modes ensures that unnecessary multicast transmissions within the mesh network are reduced and backhaul bandwidth is conserved.

The three mesh multicast modes are:

- Regular mode: In regular mode, bridging-enabled RAP and MAP multicast data across the entire mesh network and all its segments.
- In-only mode: When a MAP receives multicast packets from the Ethernet, it forwards them to the corresponding RAP's Ethernet network. No additional forwarding occurs. This setting ensures that the RAP does not send non-CAPWAP multicasts back to the MAP Ethernet networks within the mesh network (their point of origin). The system filters out MAP to MAP multicasts so these do not occur.
- In-out mode: The RAP and MAP multicast in different ways.

- If a MAP receives multicast packets over Ethernet, it sends them to the RAP. The MAP does not send these packets to other MAPs over Ethernet; the system filters MAP-to-MAP packets from the multicast stream.
- If a RAP receives multicast packets over Ethernet, it sends them to all the MAPs and their respective Ethernet networks. When in-out mode operates, partition your network to ensure a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.

Radio Resource Management on mesh

Radio resource management (RRM) features are wireless network management functions that

- enable real-time RF management of the wireless network
- monitor lightweight APs for traffic load, interference, noise, and coverage, and
- operate automatically through embedded controller software.

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

- Mesh AP has the Root AP role.
- Root AP has joined using Ethernet link.
- Root AP does not serve any child AP.

Air Time Fairness on Mesh

The Air Time Fairness (ATF) on Mesh feature is conceptually similar to the ATF feature for local access points (APs). ATF is a form of wireless quality of service (QoS) that regulates downlink airtime (as opposed to egress bandwidth). Before a frame is transmitted, the ATF budget for that SSID is checked to ensure that there is sufficient airtime budget to transmit the frame. Each SSID can be thought of as having a token bucket (1 token = 1 microsecond of airtime). If the token bucket contains enough airtime to transmit the frame, it is transmitted over air. Otherwise, the frame can either be dropped or deferred. Deferring a frame means that the frame is not admitted into the Access Category Queue (ACQ). Instead, it remains in the Client Priority Queue (CPQ) and transmitted at a later time when the corresponding token bucket contains a sufficient number of tokens (unless the CPQ reaches full capacity, at which point, the frame is dropped). The majority of the work involved in the context of ATF takes place on the APs. The wireless controller is used to configure the ATF on Mesh and display the results.

In a mesh architecture, the mesh APs (parent and child MAPs) in a mesh tree access the same channel on the backhaul radio for mesh connectivity between parent and child MAPs. The root AP is connected by wire to the controller, and MAPs are connected wirelessly to the controller. Hence, all the CAPWAP and Wi-Fi traffic are bridged to the controller through the wireless backhaul radio and through RAP. In terms of physical locations, normally, RAPs are placed at the roof top and MAPs in multiple hops are placed some distance apart from each other based on the mesh network segmentation guidelines. Hence, each MAP in a mesh tree can provide 100 percent of its own radio airtime downstream to its users though each MAP accessing the same medium. Compare this to a non-mesh scenario, where neighboring local-mode unified APs in the arena next to each other in different rooms, serving their respective clients on the same channel, and each AP

providing 100% radio airtime downstream. ATF has no control over clients from two different neighboring APs accessing the same medium. Similarly, it is applicable for MAPs in a mesh tree.

For outdoor or indoor mesh APs, ATF must be supported on client access radios that serve regular clients similarly to how it is supported on ATF on non-mesh unified local mode APs to serve the clients. Additionally, it must also be supported on backhaul radios which bridge the traffic to/from the clients on client access radios to RAPs (one hop) or through MAPs to RAPs (multiple hops). It is a bit tricky to support ATF on the backhaul radios using the same SSID/Policy/Weight/Client fair-sharing model. Backhaul radios do not have SSIDs and it always bridge traffic through their hidden backhaul nodes. Therefore, on the backhaul radios in a RAP or a MAP, the radio airtime downstream is shared equally, based on the number of backhaul nodes. This approach provides fairness to users across a wireless mesh network, where clients associated to second-hop MAP can stall the clients associated to first-hop MAP where second-hop MAP is connected wireless to first-hop MAP through backhaul radio even though the Wi-Fi users in the MAPs are separated by a physical location. In a scenario where a backhaul radio has an option to serve normal clients through universal client access feature, ATF places the regular clients into a single node and groups them. It also enforces the airtime by equally sharing the radio airtime downstream, based on the number of nodes (backhaul nodes plus a single node for regular clients).

Spectrum Intelligence for mesh

A Spectrum Intelligence feature is a wireless network monitoring capability that

- scans 2.4 GHz and 5 GHz bands for non–Wi-Fi radio interference
- provides device and air quality reports using Cisco CleanAir technology, and
- includes mitigation features like Event-Driven Radio Resource Management (EDRRM) and Persistent Device Avoidance (PDA) that require CleanAir data.

The Spectrum Intelligence feature supports both client serving and monitor modes. CleanAir technology in mesh backhaul and access radios generates Interference Device Reports (IDR) and Air Quality Index (AQI). In mesh networks, you use mitigation features with client-access radios in the same way as with non-mesh networks. However, in backhaul radios, reports are controller-only and do not trigger ED-RRM actions. You cannot enable or disable CleanAir on mesh APs (MAPs) because configuration options are not available.

For more information about Spectrum Intelligence, see Configure spectrum intelligence (CLI) section.

Indoor mesh interoperability with outdoor mesh

A mesh network is a wireless connectivity architecture that

- enables both indoor and outdoor MAPs to connect and share coverage
- allows seamless mobility groups between the two environments, and
- supports management of all MAPs through a single controller.

The system supports interoperability between indoor MAPs and outdoor APs. By default, you should use indoor MAPs inside buildings. Deploy them outside only for temporary, short-haul coverage extensions, such as connecting a building to a nearby parking lot.

You can share mobility groups between indoor and outdoor networks, and you can manage all devices with a single controller. The same WLANs that you configure can be broadcast from both indoor and outdoor MAPs.

Workgroup bridge

A workgroup bridge (WGB) is a wireless networking device that

- connects wired networks over a single wireless segment
- informs the corresponding mesh access point (MAP) of all wired clients on its segment through IAPP messages, and
- uses an additional MAC address header to route packets to and from wired clients.

Data packets for WGB clients contain an extra MAC address in the 802.11 header (four MACs, instead of the usual three), with the extra address being that of the WGB itself. The extra MAC in the header is the address of the workgroup bridge itself. This extra MAC address is used to route a packet to and from the corresponding clients.

You can configure APs as workgroup bridges. You need only one radio interface for controller connectivity. Use the Ethernet interface for wired client connectivity and another radio interface for wireless clients.

In Cisco Catalyst 9800 Series Wireless Controllers, WGB acts as a client association that allows wired clients behind the WGB to pass data over the mesh network. Wired clients with different VLANs behind a WGB are also supported.

Link test

A link test is a radio communication diagnostic tool that

- determines the radio link quality between two devices
- supports both ping and CCX test types for different directions, and
- allows both APs and clients to act as initiators and responders.

Two types of link-test packets are transmitted during a link test: request and response. Any radio that receives a link-test request packet fills in the appropriate text boxes. It then echoes the packet back to the sender with the response type set. The radio link quality in the client-to-access point direction can differ from that in the access point-to-client direction. This difference occurs because transmit power and receive sensitivity are distributed asymmetrically on both sides.

Types of link tests

The two types of link tests that you can perform are:

- **Ping link test**: With the ping link test, the controller tests link quality in the client-to-access point direction. The controller polls the RF parameters of the ping reply packets received by the AP to determine the client-to-access point link quality.
- **CCX link test**: With the CCX link test, the controller can also test the link quality in the access point-to-client direction. The controller sends link-test requests to the client. The client records RF

parameters, such as received signal strength indicator (RSSI) and signal-to-noise ratio (SNR), in the response packet. Both requestor and responder roles exist on the AP and controller. You can initiate a link test from the AP, controller, or a CCX v4 or v5 client.

Mesh daisy chaining

A mesh daisy chain is a wireless networking topology that

- connects mesh APs in series to relay data
- enables both serial backhaul communication and network extension for client access, and
- supports flexible deployment by allowing MAPs to connect in different modes and power configurations.

Mesh APs can daisy chain when operating as Mesh APs. In a daisy chain configuration, MAPs function as either serial backhaul links—using different channels for uplink and downlink to increase backhaul bandwidth—or as extensions of universal network access. Extending universal access allows a local mode or FlexConnect mode Mesh AP to connect to the Ethernet port of a MAP, expanding network reach for client devices.

Wired daisy-chained APs require specific cabling based on power source:

- If an AP uses DC power, connect an Ethernet cable from the LAN port of the Primary AP directly to the PoE-in port of the Subordinate AP.

Prerequisites for mesh Ethernet daisy chaining

Before you deploy mesh Ethernet daisy chaining, complete several configuration steps and verify specific settings on your APs. These prerequisites include designating AP roles, enabling relevant features, configuring VLAN support, and using the proper cabling to ensure optimal system performance and compatibility.

- 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 operating in bridge mode, use the **ap name** *name-of-rap* **mesh vlan-trunking [native]** *vlan-id* command. This command configures 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 4-pair cables that support 1000 Mbps. This feature does not work properly with 2-pair cables that support 100 Mbps.

Restrictions for mesh Ethernet daisy chaining

Review and meet these requirements before you configure 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.
- For Ethernet daisy chain topology, connect a power injector as the power supply for the AP. Do not connect the Cisco Industrial Wireless 3702 PoE out port to the PoE in port of another Cisco Industrial Wireless 3702 AP.
- The network convergence time increases as the number of APs in the chain increases.
- Any EWC-capable AP that is part of daisy chaining and has been assigned the RAP role must operate in CAPWAP mode (ap-type capwap).

Mesh leaf node

A mesh leaf node is a type of mesh access point (MAP) that

- operates only as a child node within a wireless mesh network
- is typically assigned to MAPs with lower performance, and
- cannot serve as a parent MAP, ensuring wireless backhaul performance is not degraded.

Leaf nodes maintain stable network throughput by preventing low-performance devices from acting as wireless backhaul links for other MAPs.

FlexConnect + bridge mode

A FlexConnect bridge mode is a wireless network configuration that

- enables FlexConnect capabilities on mesh (bridge mode) APs,
- allows mesh APs to inherit VLANs from the root AP, and
- supports VLAN trunking and native VLAN ID configuration per AP.

FlexConnect + bridge mode enables FlexConnect capabilities on mesh (bridge mode) APs. Mesh APs inherit VLANs from the root AP to which they are connected.

Any EWC-capable AP in FlexConnect 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 these modes:

- FlexConnect
- FlexConnect + bridge (FlexConnect + mesh)

Backhaul client access

Backhaul client access is a wireless networking feature that

- allows wireless clients to associate with mesh APs using the backhaul radio
- supports both 2.4 GHz and 5 GHz backhaul radios, and
- permits the backhaul radio to carry both client traffic and backhaul traffic simultaneously.

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 you enable backhaul client access, all MAPs except the subordinate AP and its child APs in a daisy-chained deployment reboot.

Mesh call admission control

A mesh call admission control is a quality of service mechanism that

- continuously monitors bandwidth available to mesh access points
- regulates voice call admissions to maintain acceptable call quality, and
- rejects calls when bandwidth or resource limits are reached.

Call Admission Control (CAC) enables a mesh AP to maintain controlled quality of service (QoS) on the controller. This management helps maintain 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 AP determines whether it can accommodate a call by checking the available bandwidth and comparing it to 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 AP rejects the call.

Mesh CAC is not supported in these scenarios.

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

Mesh network recovery mechanisms

A mesh network recovery mechanism is a network self-healing feature that

- rapidly detects uplink gateway reachability failures in mesh APs
- automatically triggers alternate uplink selection to maintain connectivity, and
- uses ICMP pings to default gateways to verify uplink status after failover events or controller disconnections.

In all 802.11ac Wave 2 and 802.11ax mesh APs, detecting uplink gateway failures quickly speeds up mesh network recovery. Mesh APs use ICMP ping to the default gateway, either IPv4 or IPv6, to check uplink gateway reachability.

Reachability checks for mesh APs work

A mesh AP triggers the reachability check in two scenarios:

- After a new uplink is selected and before the mesh AP joins the controller

  After a new uplink is selected, the mesh AP has a 45-second window to reach the gateway (through static IP or DHCP) through the selected uplink. If the mesh AP does not reach the gateway within 45 seconds, the system blocks the current uplink and starts selecting a new uplink. If the AP joins the controller during this window, it stops the reachability check. The system does not perform gateway reachability checks during normal operations.

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

  When the mesh AP times out its connection with the controller and fails to reach the gateway within 5 seconds, the system marks the current uplink as blocked and starts the uplink selection process.

Fast teardown for a mesh deployment

A fast teardown is a mesh deployment feature that

- enables rapid detection of root AP uplink failures
- helps restore or reconfigure network service when the uplink is lost, and
- applies to mesh deployments with unreliable uplinks, such as wireless microwave links.

Fast teardown for mesh APs is not supported on Cisco Industrial Wireless (IW) 3702 Access Points.

Configure MAC authorization (GUI)

Enable MAC-based authorization for wireless mesh networks. Specify which devices can connect by entering their MAC addresses.

Procedure

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

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

Step 3 In the **Quick Step: MAC Filtering** page, complete these steps:

a) Enter the **MAC Address** . The MAC address can be in either *xx:xx:xx:xx:xx:xx* , *xx-xx-xx-xx-xx-xx* , or *xxxx.xxxx.xxxx* format.
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**.

Both WebUI and CLI support MAC user configuration in these formats: xxxxxxxxxxxx, xx:xx:xx:xx:xx:xx, xx-xx-xx-xx-xx-xx, or xxxx.xxxx.xxxx. The AP sends the default MAC address without any delimiter. If the MAC address is configured with a delimiter, AP authorization fails unless it uses the xxxxxxxxxxxx format.

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** page, complete these actions:

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** page 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**.

Authorized devices with the specified MAC addresses can connect to the wireless mesh network.

Configure MAC authorization (CLI)

Enable MAC authorization for bridge mode APs by configuring the credentials and authorization methods needed.

Add the MAC address of a bridge mode AP to the controller to allow authentication.

Before you begin

- MAC filtering for bridge mode APs is enabled by default on the controller. Configure only the MAC address. Find the MAC address on the back of the AP.
- MAC authorization is supported using both internal and external AAA servers.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure username authentication for MAC filtering, using the MAC address as the username.

Example:

```
Device(config)# username user-name
```

Step 3 Set the authorization method list to use local credentials.

Example:

```
Device(config)# aaa authorization credential-download method-name local
```

Step 4 Set the authorization method list to use a RADIUS server group. The command supports up to 14 lines.

Example:

```
Device(config)# aaa authorization credential-download method-name radius group
server-group-name
```

Step 5 Configure a mesh profile to access mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh mesh-profile-name
```

Step 6 Configure the authorization method for mesh APs.

Example:

```
Device(config-wireless-mesh-profile)# method authorization method-name
```

You have successfully configured MAC authorization for bridge mode access points using the CLI on the controller.

```
Device# configure terminal
Device(config)# username username1
Device(config)# aaa authorization credential-download list1 local
Device(config)# aaa authorization credential-download auth1 radius group radius-server-1
Device(config)# wireless profile mesh mesh-profile
Device(config-wireless-mesh-profile)# method authorization auth1
```

Configure MAP authorization - EAP (GUI)

Enable secure authentication for mesh access points by configuring MAP authorization to use EAP (Extensible Authentication Protocol) through the graphical user interface (GUI).

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **AAA Method List** > **Device Authentication**.

Step 2 Click **Add**.

Step 3 Enter **Method List Name**.

Step 4 Choose **Type** as dot1x and **Group Type** from the drop-down lists.

Step 5 Check or uncheck the **Fallback to Local** check box.

Step 6 Move the required servers from the **Available Server Groups** to the **Assigned Server Groups.**

Step 7 Click **Apply to Device**.

Step 8 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 9 Click the mesh profile. The **Edit Mesh Profile** page is displayed.

Step 10 Choose the **Advanced** tab.

Step 11 In the **Security** settings, from the **Method** drop-down list, choose **EAP**.

Step 12 Choose the options from the **Authentication Method** and **Authorization Method** drop-down lists.

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

MAP authorization with EAP is now active for the selected mesh profile.

Configure MAP authorization (CLI)

Set up mesh access point (MAP) authentication for mesh access points using either Extensible Authentication Protocol (EAP) or Pre-Shared Key (PSK) methods.

Select and configure an authentication method—EAP or PSK—for MAP authentication.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Set an authentication method list to use a RADIUS server group. This is required for EAP authentication.

Example:

```
Device(config)# aaa authentication dot1x method-name radius group server-group-name
```

For local authentication:

```
Device(config)# aaa authentication dot1x auth1 local
```

Step 3 Set an authorization method list to use local credentials.

Example:

```
Device(config)# wireless profile mesh profile-name local
```

Step 4 Configure the mesh security EAP or PSK for mesh AP.

Example:

```
Device(config-wireless-mesh-profile)# security eap server-group-name
```

Step 5 Configure the authentication method for mesh AP authentication.

Example:

```
Device(config-wireless-mesh-profile)# method authentication method-name
```

You have configured MAP authorization for mesh access points using your chosen authentication method (EAP or PSK).

```
Device# configure terminal
Device(config)# aaa authentication dot1x auth1 local
Device(config)# wireless profile mesh mesh1
Device(config-wireless-mesh-profile)# security eap / psk
Device(config-wireless-mesh-profile)# method authentication auth1
```

Configure PSK provisioning (CLI)

When you enable PSK provisioning, your APs join using the default PSK. After you set the PSK provisioning key, the system pushes the configured key to each newly joined AP.

Complete these steps to configure a PSK:

Before you begin

Confirm that you have pushed the provisioned PSK to every AP 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 a total of five PSKs and one default PSK.
- A mesh AP deletes the provisioned PSK only during a factory reset.
- A mesh AP never uses the default PSK after receiving the first provisioned PSK.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the security method for wireless as PSK.

Example:

```
Device(config)# wireless mesh security psk provisioning
```

Note
The controller pushes the provisioned PSK only to APs configured with PSK as the mesh security method.

Step 3 Configure a new PSK for mesh APs.

Example:

```
Device(config)# wireless mesh security psk provisioning key index {0 | 8} preshared-key
description
```

Step 4 Enable default PSK-based authentication.

Example:

```
Device(config)# wireless mesh security psk provisioning default-psk
```

Step 5 Specify the PSK to be actively used.

Example:

```
Device(config)# wireless mesh security psk provisioning inuse index
```

Note
You should explicitly specify the in-use key index in the global configuration to point to the PSK index.

The controller provisions the specified pre-shared key on the mesh APs, sets the active key, and distributes it accordingly.

```
Device# configure terminal
Device(config)# wireless mesh security psk provisioning
Device(config)# wireless mesh security psk provisioning key 1 0 secret secret-key
Device(config)# wireless mesh security psk provisioning default-psk
Device(config)# wireless mesh security psk provisioning inuse 1
```

Configure a bridge group name (GUI)

Configure a bridge group name to organize and manage wireless mesh network profiles efficiently.

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. The MAP scans ten times to find a matching BGN parent when you enable **Strict Match** BGN.

Step 5 Click **Apply to Device**.

The system assigns and applies a new bridge group name to the mesh profile you selected.

Configure a bridge group name (CLI)

Configure a bridge group name (BGN) for a mesh profile on a wireless LAN controller using CLI commands.

- If a 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

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile and enter mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh mesh-profile-name
```

Step 3 Configure a bridge group name.

Example:

```
Device(config-wireless-mesh-profile)# bridge-group name bridge-grp-name
```

Step 4 Configure bridge group strict matching.

Example:

```
Device(config-wireless-mesh-profile)# bridge-group strict-match
```

The bridge group name is assigned to the mesh profile and applied to all associated mesh APs.

```
Device# configure terminal
Device(config)# wireless profile mesh mesh-profile-bgn
Device(config-wireless-mesh-profile)# bridge-group name bgn-grp-name
Device(config-wireless-mesh-profile)# bridge-group strict-match
```

Configure background scanning (GUI)

Enable background scanning on a wireless mesh profile to improve network performance and reliability.

Procedure

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

Step 2 Select your desired profile.

Step 3 In **General** tab, check the **Background Scanning** check box.

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

You have activated background scanning for the selected wireless mesh profile.

Configure background scanning

To enable background scanning in mesh deployments so that mesh access points (MAPs) can detect neighboring channels and identify better parent nodes, maintaining optimal uplink connections.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile and enter the mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh mesh-profile-name
```

Step 3 Configure background scanning to enable mesh access points to find better parent nodes and maintain optimal connections.

Example:

```
Device(config-wireless-mesh-profile)# background-scanning
```

Background scanning is enabled in the mesh profile. Mesh APs scan neighboring channels to find better parent nodes. This helps maintain optimal uplink performance in the mesh network.

```
Device# configure terminal
Device(config)# wireless profile mesh mesh-profile-name
Device(config-wireless-mesh-profile)# background-scanning
```

Configure AP fast ancestor find mode (GUI)

Enable a child MAP to synchronize with any neighbor parent MAP across all channels.

Use the GUI to configure the MAP Fast Ancestor Find feature within a mesh profile.

Follow these steps to configure AP fast ancestor find mode through the GUI:

Procedure

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

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

Step 3 In the **Add Mesh Profile** page, 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.

The MAP Fast Ancestor Find feature is enabled for the specified mesh profile.

Configure background scanning and MAP fast ancestor find mode (Task)

Configure background scanning and MAP fast ancestor find mode using the CLI within a mesh profile for detailed configuration options.

Follow these steps to configure background scanning and MAP fast ancestor find mode through the CLI:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile and enter mesh profile configuration mode.

Example:

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

Step 3 Enable background scanning in mesh deployments.

Example:

```
Device(config-wireless-mesh-profile)# background-scanning
```

Note
In Cisco Catalyst 9124 Series Access Points, a dedicated RF ASIC radio is used for background scanning.

Step 4 Enable fast ancestor find mode.

Example:

```
Device(config-wireless-mesh-profile)# map-fast-ancestor-find
```

Background scanning and MAP fast ancestor find mode are enabled for the specified mesh profile.

Example

```
Device# configure terminal
Device# wireless profile mesh default-mesh-profile
```

```
Device(config-wireless-mesh-profile)# background-scanning
Device(config-wireless-mesh-profile)# map-fast-ancestor-find
```

Configure backhaul client access (GUI)

Enable backhaul client access for mesh device profiles.

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**.

The system updates the profile and enables backhaul client access for devices that use the selected mesh profile.

Configure backhaul client access (CLI)

Enable backhaul client access on a mesh profile. This allows client devices to connect to the APs through the mesh backhaul. The result is increased network flexibility and coverage.

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

Complete these steps to enable backhaul client access on a mesh profile:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile and enter mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh profile-name
```

Step 3 Configure backhaul with client access AP.

Example:

```
Device(config-wireless-mesh-profile)# client-access
```

You have enabled backhaul client access on the selected mesh profile.

```
Device# configure terminal
Device(config)# wireless profile mesh profile-name
Device(config-wireless-mesh-profile)# client-access
```

Configure dot11ax rates on mesh backhaul per AP (GUI)

This task enables you to configure specific dot11ax (Wi-Fi 6) rates for mesh backhaul connections on individual APs.

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 Select the mesh AP that has been configured.
The **Edit AP** page 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 the 802.11a/b/g/n/ac/ax rates, depending on the AP. The Cisco Catalyst 9124AX Outdoor AP is the only AP that supports 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 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**.

After you complete the steps, the selected mesh access point operates using the configured dot11ax rates for its backhaul link.

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**.

Configure wireless backhaul data rate (CLI)

Configure the data transmission rate for wireless backhaul connections between APs using CLI commands to optimize wireless network performance, coverage, and spectrum use.

Use backhaul to create a wireless connection between APs. Depending on the AP, the backhaul interface can be 802.11bg, 802.11a, 802.11n, or 802.11ac. Selecting a rate lets you use the available RF spectrum effectively.

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 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 this procedure to configure wireless backhaul data rate in privileged EXEC mode or in mesh profile configuration mode.

Procedure

Step 1 Enter privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 Configure backhaul transmission rate.

Example:

```
Device# ap name ap-name mesh backhaul rate {auto | dot11abg | dot11ac | dot11n}
```

Step 3 Configure a mesh profile and enter mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh profile-name
```

Step 4 Configure backhaul transmission rate.

Example:

```
Device(config-wireless-mesh-profile)# backhaul rate dot11  { 24ghz | 5ghz | 6ghz} dot11n
RATE_6M
```

Note
Ensure the rate you configure on the AP (step 2) matches the rate you configure on the mesh profile (step 4).

After you configure the wireless backhaul data rate, your APs will balance coverage area and performance for your deployment.

```
Device> enable
Device# ap name ap1 mesh backhaul rate auto
Device(config)# wireless profile mesh mesh1
Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11n mcs 31
```

Configure data rate per AP (CLI)

Configure data transmission rates for each AP on mesh backhaul for the 2.4 GHz and 5 GHz bands using the command-line interface.

Procedure

Step 1 Enter privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 Configure the 802.11ax mesh backhaul rates for the 2.4 GHz and 5 GHz bands.

Example:

```
Device# ap name ap-name mesh backhaul rate dot11ax mcs <0-11> ss <1-8>
```

The AP uses the configured backhaul data rates for 2.4 GHz and 5 GHz bands.

```
Device> enable
Device# ap name ap-name mesh backhaul rate dot11ax mcs 5 ss 4
```

Configure data rate using mesh profile (CLI)

Set specific data rates for 2.4 GHz and 5 GHz backhaul communication in mesh profiles to optimize wireless mesh network performance.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile and enter mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh profile-name
```

Step 3 Configure the backhaul transmission rate for the 2.4 GHz band and the 5 GHz band. For the 2.4 GHz band, set the 802.11ax spatial stream value from 1 to 4. For the 5 GHz band, set the spatial stream value from 1 to 8.

Example:

```
Device(config-wireless-mesh-profile)# backhaul rate dot11 {24ghz | 5ghz} dot11ax mcs <0-11>
 spatial-stream <1-8>
```

The mesh profile is updated with the configured data rate for the specified frequency band and spatial streams.

```
Device# configure terminal
Device(config)# wireless profile mesh profile-name
Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11ax mcs 5 spatial-stream
 6
```

Configure mesh backhaul (CLI)

Set the mesh backhaul frequency for an access AP using CLI commands.

Procedure

Change the mesh backhaul to 2.4 GHz.

Example:

```
Device # ap name test-ap mesh backhaul radio dot11 24ghz
```

The specified access point now uses 2.4 GHz as its mesh backhaul radio frequency.

Configure dynamic frequency selection (CLI)

Configure dynamic frequency selection (DFS) on your device to enable radar detection and meet DFS requirements.

DFS specifies the types of radar waveforms that should be detected and the timers that must be used for operation in the DFS channel.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile and enter mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh profile-name
```

Step 3 Enable DFS.

Example:

```
Device(config-wireless-mesh-profile)# full-sector-dfs
```

Note
DFS functionality allows a MAP that detects a radar signal to transmit this information to the RAP. The RAP treats this as a radar detection and moves the sector. This process is called the coordinated channel change. The coordinated channel change feature is always enabled on Cisco Wave 2 and newer APs. You can disable this feature only on Cisco Wave 1 APs.

Dynamic Frequency Selection is enabled for your mesh profile. Your mesh profile is now ready to operate and meets radar detection requirements.

```
Device# configure terminal
Device(config)# wireless profile mesh dfs-mesh-profile
Device(config-wireless-mesh-profile)# full-sector-dfs
```

Configure the intrusion detection system (CLI)

Enable intrusion detection system monitoring and reporting on mesh APs to enhance network security.

When enabled, the intrusion detection system generates reports for all client access traffic. This feature does not apply to backhaul traffic.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile and enter mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh profile-name
```

Step 3 Configure intrusion detection system reporting for mesh APs.

Example:

```
Device(config-wireless-mesh-profile)# ids
```

The device is now configured to report intrusion detection events for mesh APs.

```
Device# configure terminal
Device(config)# wireless profile mesh mesh-ids
Device(config-wireless-mesh-profile)# ids
```

Configure Ethernet bridging (GUI)

Enable Ethernet bridging on a mesh profile so that network traffic can be transparently passed between Ethernet segments.

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**.

Ethernet bridging is now enabled for the selected mesh profile.

Configure Ethernet bridging (CLI)

Configure Ethernet bridging on mesh access points (APs) to allow Ethernet devices to connect through AP ports.

The Ethernet ports on MAPs are disabled by default. To enable them, configure Ethernet bridging on the Root AP and the relevant MAPs.

You can enable Ethernet bridging to:

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

Before you begin

- Ensure that you configure these 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. VLAN filtering is allowed with this AP command: **[no] mesh ethernet** { **0** | **1** | **2** | **3** } **mode trunk vlan allowed** .

Note If you want all VLANs bridged (the bridge acts like a piece of wire), enable VLAN transparency to allow all VLANs to pass. To avoid unnecessary traffic flooding the network, filter VLANs on the wired side when using VLAN transparent mode.

- Configure the switch port that connects to the root AP as a trunk port so Ethernet bridging works.
- 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. You must configure this command to enable the Ethernet Bridging feature on the AP.
- For FlexConnect+Bridge APs, configure the native VLAN ID under the corresponding flex profile.

e

Note To ensure that the MAPs apply the Ethernet VLAN configuration on the controller, configure the native VLAN on the RAP by running this command:

```
Device# ap name ap-name no mesh vlan-trunking
Device# ap name ap-name mesh vlan-trunking native 247
```

Alternatively, you can configure native VLAN on the RAP and then the MAP in this order:

```
Device# ap name ap-name no mesh vlan-trunking
Device# ap name ap-name mesh vlan-trunking native vlan_id
Device# ap name ap-name mesh ethernet 1 mode trunk vlan native native
Device# ap name ap-name mesh ethernet 0 mode trunk vlan allowed allowed
```

To verify the status of RAP and MAP, run this command:

```
Device# show mesh forwarding all
```

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
Device> enable
```

Enter your password, if prompted.

Step 2 Configure the Ethernet port of the AP and set the mode.

Example:

```
Device# ap name ap-name mesh ethernet {0 | 1 | 2 | 3} mode access vlan-id
```

Step 3 Set the native VLAN for the trunk port.

Example:

```
Device# ap name ap-name mesh ethernet {0 | 1 | 2 | 3} mode trunk vlan native 21
```

Step 4 Configure the allowed VLANs for the trunk port.

Example:

```
Device# ap name ap1 mesh ethernet  { 0 | 1 | 2 | 3 } mode trunk vlan allowed vlan-id
```

This command permits VLAN filtering on an Ethernet port of any Mesh or Root Access Point. It is active only when VLAN transparency is disabled in the mesh profile.

Ethernet bridging is enabled on the AP, allowing devices to communicate through configured VLANs.

```
Device> enable
Device# ap name ap1 mesh ethernet 1 mode access 21
Device# ap name ap1 mesh ethernet 1 mode trunk vlan native 21
Device# ap name ap1 mesh ethernet 1 mode trunk vlan allowed 21
```

Configure multicast modes over mesh

Enable multicast forwarding behavior so that your wireless mesh network operates efficiently.

- If multicast packets are received at a MAP over Ethernet, the MAP sends them to the RAP. The MAP does not send them to other MAPs; it filters out MAP-to-MAP packets from 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. To prevent a multicast sent by one RAP from being received by another RAP on the same Ethernet segment and then sent back into the network, properly partition your network when the *in-out* mode is in operation.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile and enter mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh profile-name
```

Step 3 Configure mesh multicast mode.

Example:

```
Device(config-wireless-mesh-profile)# multicast {in-only | in-out | regular}
```

You have set the mesh profile to the multicast mode you want. This setting controls how multicast packets are routed in the network.

```
Device# configure terminal
Device(config)# wireless profile mesh mesh-multicast
Device(config-wireless-mesh-profile)# multicast regular
```

Configure RRM on mesh backhaul (CLI)

RRM measurement in the mesh AP backhaul is enabled if your access point meets these conditions:

- Mesh AP has the Root AP role.
- The Root AP has joined the network using an Ethernet link.
- Root AP does not serve any child AP.

Complete the steps to enable RRM in the mesh backhaul:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure RRM on the mesh backhaul.

Example:

```
Device(config)# wireless mesh backhaul rrm
```

RRM is enabled on the mesh backhaul for APs.

```
Device# configure terminal
Device(config)# wireless mesh backhaul rrm
```

Configure RRM channel assignment for root access points globally

Configure Radio Resource Management (RRM) channel assignment policies for all root access points. This configuration optimizes wireless performance, minimizes interference, and maintains network stability across your deployment.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure RRM for mesh backhaul.

Example:

```
Device(config)# wireless mesh backhaul rrm
```

Step 3 (Optional) Configure auto DCA for RF Application Specific Integrated Circuit (ASIC) integrated RAPs.

Example:

```
Device(config)# wireless mesh backhaul rrm auto-dca
```

All RAPs adopt the configured RRM channel assignment settings globally. This change results in improved channel distribution, reduced interference, and more reliable wireless connectivity across the network.

```
Device# configure terminal
Device(config)# wireless mesh backhaul rrm
Device(config)# wireless mesh backhaul rrm auto-dca
```

Complete these steps to configure the initial channel assignment of the RAP in privileged EXEC mode through RRM and to initiate channel selection for each bridge group.

Procedure

	Command or Action	Purpose
Step 1	Enter privileged EXEC mode. **Example:** `Device> enable`	
Step 2	Initiate the update of the 802.11, 802.11a, or 802.11b channel selection for every mesh Cisco AP. **Example:** `Device# ap dot11 {24ghz | 5ghz | 6ghz} rrm channel-update mesh`	
Step 3	Initiate the update of the 802.11, 802.11a, or 802.11b channel selection for mesh AP in the bridge group. **Example:** `Device# ap dot11 {24ghz | 5ghz | 6ghz} rrm channel-update mesh bridge-group` *`bridge-group-name`*	

RRM completes the channel assignment for the RAP in privileged EXEC mode.

```
Device> enable
Device# ap dot11 5ghz rrm channel-update mesh
Device# ap dot11 5ghz rrm channel-update mesh bridge-group cisco-bridge-group
```

Configure RRM channel assignment for an AP

Assign RRM channels to an AP. This action helps you optimize wireless channel usage and reduce interference.

Procedure

Step 1 Enter privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 Trigger the RRM DCA process for your AP.

Example:

```
Device# ap name Cisco-ap-name dot11 {24ghz | 5ghz | 6ghz} rrm channel update mesh
```

After you trigger the process, the system starts the RRM DCA process and updates the channel assignment for your selected radio band.

```
Device> enable
Device# ap name Cisco-ap-name dot11 5ghz rrm channel update mesh
```

Select a preferred parent (GUI)

Direct a mesh-capable AP to use a designated parent for uplink within the wireless topology.

Procedure

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

Step 2 Click the AP.

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

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

The AP uses the specified preferred parent MAC address for uplink, optimizing connectivity in the mesh network.

Select a preferred parent (CLI)

To configure a preferred parent for a MAP, complete these steps.

You can override the AWPP-defined parent selection and assign a specific preferred parent to a mesh AP using this mechanism.

Procedure

Step 1 Enter privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 Configure mesh parameters for the AP and set the mesh-preferred parent MAC address.

Example:

```
Device# ap name ap-name mesh parent preferred mac-address
```

Note
Ensure that you use the radio MAC address of the preferred parent.

For Cisco Wave 1 APs, specify the MAC address of the actual mesh neighbor as the preferred parent. Use the base radio MAC address that ends with the letter "f". 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, specify the MAC address for the preferred parent by adding "0x11" to the last two characters of the base radio MAC address. 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
```

The mesh AP is configured to use the specified MAC address as its preferred parent.

```
Device> enable
Device# ap name ap1 mesh parent preferred 00:0d:ed:dd:25:8F
```

Change the role of an AP (GUI)

Change the operational role of an AP to support different network topologies.

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** .

The AP automatically restarts to apply the new role configuration.

Change the role of an AP (CLI)

Change your Cisco access point (AP) role between mesh AP (MAP) and root AP (RAP) using command-line interface (CLI) commands.

To change the AP from MAP to RAP or the reverse, follow this procedure. By default, your AP joins the controller in the mesh AP role.

Procedure

Step 1 Enter privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 Change the role of the Cisco bridge mode AP. The AP reboots after the role change.

Example:

```
Device# ap name ap-name role {mesh-ap | root-ap}
```

The specified AP reboots and operates in its new role. After rebooting, it connects and functions in your wireless mesh network.

```
Device> enable
Device# ap name ap1 role root-ap
```

Configure mesh leaf node (CLI)

Set an AP as a mesh leaf node. Other mesh APs cannot select this AP as a parent MAP.

Procedure

Step 1 Enter privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 Configure the AP to operate only as a leaf node. Other MAPs cannot select this AP as a parent MAP.

Example:

```
Device# ap name ap-name mesh block-child
```

Use the **no** form of this command to change it to a regular AP.

The AP operates solely as a mesh leaf node and cannot be selected as a parent MAP.

```
Device> enable
Device# ap name ap1 mesh block-child
```

Configure the mesh leaf node (GUI)

Configure a mesh leaf node so that it blocks child connections to enforce network segmentation.

Procedure

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

Step 2 Click the AP.

Step 3 In the **Mesh** tab, check the **Block Child** check box.

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

Your mesh leaf node now blocks child connections.

Configure subset channel synchronization

Enable synchronization of mesh subset channels to ensure efficient convergence of RAPs and MAPs.

The controller sends all channels used by RAPs to MAPs for future seeking and convergence. The controller keeps a list of subset channels for each Bridge Group Name (BGN) and shares this list across all controllers in a mobility group.

The subset channel list includes channels where RAPs within a Bridge Group Name (BGN) operate. This list is distributed to all mesh access points (MAPs) within controllers and across controllers. Maintaining a subset channel list helps Mesh APs converge faster. You can select the convergence method in the mesh profile. The system sends the subset channel list to MAPs if the convergence method is non-standard.

Follow these steps to configure subset channel synchronization for a mobility group.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure subset channel synchronization for a mobility group.

Example:

```
Device(config)# wireless mesh subset-channel-sync mac
```

The mobility group synchronizes subset channels, which enables mesh APs to converge faster.

```
Device# configure terminal
Device(config)# wireless mesh subset-channel-sync mac
```

Provision LSC for bridge-mode and mesh APs (GUI)

Provision LSCs. This action secures communication for bridge-mode and mesh APs.

Procedure

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

Step 2 In the **Add APs to LSC Provision List** settings, click the **Select File** option to upload a CSV file that contains AP details.

Step 3 Click **Upload File**.

Step 4 You can also use the **AP MAC Address** field to search for APs by MAC address and add them. The system displays APs added to the provision list in the **APs in Provision List** list.

Step 5 Click **Apply**.

Step 6 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 7 Click **Add**.

Step 8 In the **General** tab, enter the **Name** of the mesh profile and check the **LSC** check box.

Step 9 In the **Advanced** tab, under the **Security** settings, choose the authorization method from the **Authorization Method** drop-down list.

Step 10 Click **Apply to Device**.

The system successfully applies LSC provisioning to the specified bridge-mode and mesh APs.

Provision LSC for bridge-mode and mesh APs

- Configuring a Locally Significant Certificate (LSC) will not remove preexisting certificates from an AP.
- An AP can have both LSC and Message Integrity Check (MIC) certificates. However, when you provision an AP with LSC, the MIC certificate is not used when the AP starts. If you switch from LSC to MIC, reboot the AP.

To configure LSC for bridge-mode and mesh APs, use this procedure:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure LSC provisioning for an AP.

Example:

```
Device(config)# ap lsc-provision
```

Note
This step is applicable only for mesh APs.

Step 3 (Optional) Configure LSC provisioning for all APs in the provision list.

Example:

```
Device(config)# ap lsc-provision provision-list
```

Step 4 Configure a named authorization list to download EAP credentials from the RADIUS group server.

Example:

```
Device(config)# aaa authentication dot1x auth-list radius group radius-server-grp
```

Step 5 Create a mesh profile to enter mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh mesh-profile-name
```

Step 6 Set mesh security for LSC-only MAP authentication.

Example:

```
Device(config-wireless-mesh-profile)# lsc-only-auth
```

All the mesh APs reboot after you run this command.

Step 7 Configure an authorization method for mesh APs.

Example:

```
Device(config-wireless-mesh-profile)# method authorization local
```

All bridge-mode and mesh APs are provisioned with Locally Significant Certificates (LSC).

```
Device# configure terminal
Device(config)# ap lsc-provision
Device(config)# ap lsc-provision provision-list
Device(config)# aaa authentication dot1x list1 radius group sg1
Device(config)# wireless profile mesh mesh1
Device(config-wireless-mesh-profile)# lsc-only-auth
Device(config-wireless-mesh-profile)# method authorization list1
```

Specify the backhaul slot for the root AP (GUI)

Configure the backhaul slot for a root access point to optimize wireless mesh connectivity and ensure reliable network communication.

Procedure

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

Step 2 Click **Add**.

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

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

Step 5 Click **Apply to Device**.

The system updates the root access point with the specified backhaul slot settings. It uses the selected rate types for 5 GHz and 2.4 GHz band backhaul connections.

Specify the backhaul slot for the root AP (CLI)

Assign a specific radio slot (2.4 GHz or 5 GHz) to the mesh backhaul of your root access point to optimize wireless connectivity and network performance.

Procedure

Step 1 Enter privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 Specify the mesh backhaul radio slot for your root AP.

Example:

```
Device# ap name ap-name mesh backhaul radio dot11 {24ghz | 5ghz} [slot slot-id]
```

Assign a radio slot (2.4 GHz or 5 GHz) to the mesh backhaul of your root access point to improve wireless connectivity and network performance.

```
Device> enable
Device# ap name rap1 mesh backhaul radio dot11 24ghz slot 2
```

Use a link test on mesh backhaul (GUI)

Network administrators can validate wireless mesh backhaul connectivity and signal strength with this task. Running a link test enables proactive identification of performance issues, ensures reliable mesh network operation, and helps troubleshoot weak connections.

Procedure

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

Step 2 Select the Access Point.

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

Step 4 Select 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**.

You can see the detailed link test results for the selected mesh backhaul connection.

Use a link test on mesh backhaul

To initiate a link test between neighbor mesh APs, complete these steps.

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

Step 1 Enters privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 Set the link test parameters.

Example:

```
Device# ap name ap-name mesh linktest H.H.H data-rate packet-per-sec packet-size test-duration
```

- *H.H.H*: Specify the destination AP MAC address.
- *data-rate*: Specify the data rates in Mbps. The values are 1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54, 108, or m0 through m15.
- *packet-per-sec*: Specify the packets to be sent per second. The range is from 1 to 25,000.
- *packet-size*: Specify the packet size in bytes. The range is from 1 to 1,500.
- *test-duration*: Specify the test duration in seconds. The range is from 10 to 300.

The system displays test results, including throughput, loss, and latency metrics, to verify link quality between access points.

```
Device> enable
Device# ap name ap1 mesh linktest F866.F267.7DFB 24 234 1200 200
```

Configure battery state for mesh AP (GUI)

Configure the battery state on a mesh AP using the web interface.

Procedure

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

Step 2 Select a profile.

Step 3 On the **General** tab, check the **Battery State for an AP** check box.

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

After you configure the profile, the profile displays the battery state for the selected mesh AP.

Configure battery state for mesh AP (CLI)

Some outdoor APs come with the option of battery backup. The AP also includes a POE-out port that powers a video surveillance camera. The integrated battery provides temporary backup power during external power interruptions.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile, and enter mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh profile-name
```

Step 3 Configure the battery state for an AP.

Example:

```
Device(config-wireless-mesh-profile)# battery-state
```

You have configured the battery state for the mesh AP, so backup power is now available when required.

```
Device# configure terminal
Device(config)# wireless profile mesh mesh-profile-name
Device(config-wireless-mesh-profile)# battery-state
```

Configure mesh convergence (CLI)

This section provides information about how to configure mesh convergence.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a mesh profile.

Example:

```
Device(config)# wireless profile mesh profile-name
```

Step 3 Configure mesh convergence method in a mesh profile.

Example:

```
Device(config-wireless-mesh-profile)# convergence {fast | noise-tolerant-fast | standard |
 very-fast}
```

You have successfully configured mesh convergence for the specified mesh profile on the device.

```
Device# configure terminal
Device(config)# wireless profile mesh mesh1
Device(config-wireless-mesh-profile)# convergence fast
```

Configure DHCP server on root AP (CLI)

Configure a DHCP server on the root AP.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure an AP profile.

Example:

```
Device(config)# ap profile ap-profile-name
```

Step 3 Configure the DHCP server on the root AP.

Example:

```
Device(config-ap-profile)# dhcp-server
```

Step 4 **end**

Example:

```
Device(config-ap-profile)# end
```

The system saves the configuration, exits configuration mode, and returns to privileged **EXEC** mode.

The root AP is now configured as a DHCP server and assigns IP addresses to associated clients.

Configure mesh Ethernet daisy chaining (CLI)

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

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Specify the AP profile.

Example:

```
Device(config)# ap profile default-ap-profile
```

Step 3 Configure persistent SSID broadcast and ensure strict wired uplink. RAP will not switch to wireless backhaul when you configure this command.

Example:

```
Device(config-ap-profile)# ssid broadcast persistent
```

Mesh Ethernet daisy chaining is successfully enabled on the mesh AP. The SSID broadcast is persistent and the RAP uses a strict wired uplink.

Enable mesh Ethernet daisy chaining

This section describes how to enable the Mesh Ethernet Daisy Chaining feature on a Cisco IW 3702 AP.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a mesh profile.

Example:

```
Device(config)# wireless profile mesh default-mesh-profile
```

Step 3 Connect remote wired networks to each other.

Example:

```
Device(config)# ethernet-bridging
```

Step 4 Disable VLAN transparency to ensure that the bridge is VLAN aware.

Example:

```
Device(config)# no ethernet-vlan-transparent
```

The Ethernet daisy chaining feature is enabled.

Configure mesh CAC (CLI)

Enable mesh CAC to manage call admission and ensure quality over wireless mesh links.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable mesh CAC mode.

Example:

```
Device(config)# wireless mesh cac
```

Mesh CAC is activated. Only the supported number of concurrent calls can occur over mesh links, which preserves call quality.

Configure ATF on mesh (GUI)

Configure ATF to optimize bandwidth allocation among clients on a mesh network.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Airtime Fairness** > **Global Config**.

Step 2 For **5 GHz Band** and **2.4 GHz Band**, enable the **Status** and the **Bridge Client Access** toggle button.

Step 3 To select the **Mode**, click the **Monitor** or **Enforced** radio button.

Step 4 Enable or disable the **Optimization** toggle button.

Step 5 Enter **Airtime Allocation**.

Step 6 Click **Apply to Device**.

The ATF settings are applied and mesh APs operate with the new airtime fairness parameters.

Configure ATF on mesh

Ensure fair airtime allocation and optimize wireless performance for mesh environments.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure an RF profile to enter RF profile configuration mode.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6gh} rf-profile rf-profile1
```

Step 3 Configure airtime allocation weight percentage for mesh APs.

Example:

```
Device(config-rf-profile)# airtime-fairness bridge-client-access airtime-allocation
allocation-weight-percentage
```

You have now configured mesh APs for ATF. Balanced airtime allocation improves wireless network efficiency.

```
Device# configure terminal
Device(config)# ap dot11 24ghz rf-profile rfprof24_1
Device(config-rf-profile)# airtime-fairness bridge-client-access airtime-allocation 10
```

Create an ATF policy for a MAP

Define and enable an Airtime Fairness (ATF) policy for a Mesh Access Point (MAP). This policy optimizes wireless network performance and ensures equitable airtime distribution among connected clients.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure WLAN policy profile to enter wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy  rr-xyz-policy-1
```

Step 3 Enable ATF in the existing RF profile.

Example:

```
Device(config-wireless-policy)# dot11 24ghz airtime-fairness atf-policy
```

Airtime Fairness is applied to the specified MAP when the policy is enabled.

```
Device# configure terminal
Device(config)# wireless profile policy rr-xyz-policy-1
Device(config-wireless-policy)# dot11 24ghz airtime-fairness atf-policy1
```

Create an ATF policy (GUI)

Create a new Air Time Fairness (ATF) policy and apply it to a MAP (Managed Access Point) for optimal client traffic sharing.

Procedure

Step 1 Choose **Configuration** > **Air Time Fairness** > **Profiles**.

Step 2 On the **Profiles** window, click **Add**.

Step 3 In the **Add ATF Policy** window, specify a name, ID, and weight for the ATF policy.

Note
A weighted ratio is used instead of percentages, allowing the total to exceed 100. The minimum weight that you can set is 5.

Step 4 Use the slider to enable or disable the **Client Sharing** feature.

Step 5 Click **Save & Apply to Device** to save your ATF configuration.

Step 6 (Optional) To delete a policy, check the check box next to the appropriate policy and click **Delete**.

Step 7 (Optional) To edit an existing ATF policy, select the check box next to the policy you want to edit.

In the **Edit ATF Policy** window that is displayed, you can modify the weight and client sharing details for the policy.

You have created and applied the new ATF policy to the selected MAP.

Add an ATF to a policy profile (GUI)

Enable ATF on your selected policy profiles to assign fair radio resource allocation policies to wireless clients.

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Policy**.

Step 2 Click the name of your policy profile.

Step 3 Click the **Advanced** tab.

Step 4 In the **Air Time Fairness Policies** section, choose the appropriate status for the 2.4 GHz Policy and 5 GHz Policy.

Step 5 Click **Update & Apply to Device**.

Your selected policy profile is updated and now includes the ATF settings you chose.

Enable ATF mode in an RF profile (GUI)

Enable Airtime Fairness mode to distribute wireless bandwidth more equitably among clients in an RF profile.

Procedure

Step 1 Choose **Configuration > Tags & Profiles > RF**.

Step 2 Click the name of the corresponding RF profile.

Step 3 In the **RF Profile** window, click the **Advanced** tab.

Step 4 In the **ATF Configuration** section, choose the appropriate status:

- **Status**: If you choose **Enabled** as the status, select the **Mode** as either **Monitor** or **Enforced**. You can also enable or disable optimization for this mode.
- **Bridge Client Access**
- **Airtime Allocation**: Enter the allocation value. You can set the value only after you enable the **Bridge Client Access**.

Step 5 Click **Update & Apply to Device**.

ATF mode is enabled for the selected RF profile, and the corresponding settings are applied to the device.

Enable wireless mesh profile (CLI)

To enable and configure a wireless mesh profile to support mesh networking functionality on your device.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile and enter mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh profile-name
```

Step 3 Enable the fast teardown of mesh network and configure the parameters of the feature.

Example:

```
Device(config-wireless-profile-mesh)# fast-teardown
```

The wireless mesh profile is enabled and configured with the fast teardown feature.

```
Device# configure terminal
Device(config)# wireless profile mesh mesh1
Device(config-wireless-profile-mesh)# fast-teardown
```

Enable serial backhaul in radio profile (GUI)

Enable mesh backhaul features on a specific radio profile to support serial backhaul in mesh deployments.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF/Radio** > **Radio**.

Step 2 Click **Add** to add a radio profile.
The **Add Radio Profile** page is displayed.

Step 3 In the **Add Radio Profile** page, enter the name, and description.

Step 4 In the **Mesh Backhaul** field, choose the **Enabled** radio button to enable the feature.

Step 5 In the **Mesh Designated Downlink** field, choose the **Enabled** radio button to enable the feature.

Note
Mesh Designated Downlink is supported only on slot number 2 of Mesh APs. Radio profiles must be matched carefully to RF tag slots.

Step 6 Click **Apply to Device**.

The radio profile is updated, enabling serial backhaul for selected mesh APs.

Enable mesh configurations in radio profile (CLI)

Configure your Cisco wireless AP to enable mesh backhaul and designate downlink radio slots in a radio profile.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure wireless radio profile and enter the radio-profile configuration mode.

Example:

```
Device(config)# wireless profile radio radio-profile-name
```

Step 3 Enable mesh backhaul.

Example:

```
Device(config-wireless-radio-profile)# mesh backhaul
```

By default, this command is enabled. Mesh backhaul can be disabled on a specific slot, to stop the specific slot from being the backhaul candidate.

Step 4 Enable the radio slot as a designated downlink.

Example:

```
Device(config-wireless-radio-profile)# mesh designated downlink
```

By default, this command is disabled. It is enabled only for slot 2 of mesh APs. If another slot is configured as the designated downlink, a warning message appears: `Designated downlink is supported only on slot 2 of mesh APs. Associate in the RF tag accordingly.`

By default, all the radio slots are mesh-enabled and not designated as downlink.

The mesh backhaul and designated downlink configurations are now applied to your selected radio profile.

Enable serial backhaul (CLI)

Configure a wireless profile to designate a radio as a mesh downlink backhaul.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the wireless RF tag to enter wireless RF tag profile configuration mode.

Example:

```
Device(config)# wireless profile radio radio-profile-name
```

Step 3 Enable the specified radio as a designated mesh downlink backhaul.

Example:

```
Device(config-wireless-radio-profile)# mesh designated downlink
```

The designated downlink is enabled in the radio profile only for slot 2.

Step 4 Exit the submode and return to global configuration mode.

Example:

```
Device(config-wireless-radio-profile)# exit
```

Step 5 Configure the wireless RF tag to enter wireless RF tag profile configuration mode.

Example:

```
Device(config)# wireless tag rf rf-profile-name
```

The designated downlink is enabled in the radio profile only for slot 2.

Step 6 Configure the designated downlink radio for serial backhaul.

Example:

```
Device(config-wireless-rf-tag)# dot11 5ghz {slot1 | slot2} radio-profile radio-profile-name
```

Note
In mesh APs, the uplink and downlink are in the same slot by default. When you configure a designated downlink, the mesh AP is forced to use a specific radio as downlink.

The specified radio is now configured as a designated mesh downlink, and the mesh AP is forced to use that radio for downlink backhaul.

Fallback Mode

Note If you configure at least one radio as a designated downlink, that radio will not be available for uplink. To prevent a configuration mistake, such as configuring the uplink radio as the designated downlink, the mesh AP uses a fallback timer. If the mesh AP cannot join the controller within 10 minutes, the designated configurations are cleared, and all radios become uplink-capable.

```
Device# configure terminal
Device(config)# wireless profile radio radio-mesh-downlink
Device(config-wireless-radio-profile)# mesh designated downlink
Device(config-wireless-radio-profile)# exit
Device(config)# wireless tag rf radio profile rf-map-tag
Device(config-wireless-rf-tag)# dot11 5ghz slot2 radio-profile radio-mesh-downlink
```

Mesh serial backhaul - configuration example

This example explains how to configure mesh APs to allow only slot 0 and slot 1 for backhaul connectivity:

```
Device# configure terminal
Device(config)# wireless profile radio radio-mesh-downlink
Device(config-wireless-radio-profile)# no mesh backhaul
Device(config-wireless-radio-profile)# exit

Device(config)# wireless tag rf rf-map-tag
Device(config-wireless-rf-tag)# dot11 5ghz slot2 radio-profile mesh-disabled
```

Associate wireless mesh to an AP profile (CLI)

Associate a mesh profile with an AP profile to enable mesh capabilities on compatible APs through CLI configuration.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the AP profile to enter AP profile configuration mode.

Example:

```
Device(config)# ap profile default-ap-profile
```

Step 3 In AP profile configuration mode, configure the mesh profile.

Example:

```
Device(config-ap-profile)# mesh-profile mesh-profile-name
```

The AP profile now uses the specified mesh profile. All APs using this profile inherit mesh configuration parameters.

```
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# mesh-profile test1
```

Configure fast teardown for a mesh AP profile (GUI)

Use this procedure to configure mesh AP profiles for rapid detection of uplink failures and improve mesh network resiliency.

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, an authentication method, and an authorization method.

Step 5 Enable **Ethernet bridging** if it is required.

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

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

Step 8 Perform these actions in the **Fast Roaming** section:

- Check the **Fast Teardown** check box to detect the root AP 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 from 1 to 10.
- In the **Interval value** field, enter the retry value. The valid range is from 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 from 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 from 1 to 30 seconds.
- In the **Uplink Recovery Interval** field, enter the time during which root AP uplink must be stable in order to accept the child connections. The valid range is from 1 and 3600 seconds.

Step 9 Click **Apply to Device**.

Your mesh AP profile now supports fast teardown. This configuration enables the system to detect uplink failures more quickly, helping your devices recover rapidly.

Configure fast teardown for a mesh AP profile (CLI)

Enable and configure fast teardown for a mesh AP profile to reduce network restoration time and increase network reliability.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile and enter the mesh profile configuration mode.

Example:

```
Device(config)# wireless profile mesh profile-name
```

Step 3 Enable the fast teardown of mesh network and configure the feature's parameter.

Example:

```
Device(config-wireless-mesh-profile)# fast-teardown
```

Step 4 Enable the fast teardown feature.

Example:

```
Device(config-wireless-mesh-profile-fast-teardown)# enabled
```

Step 5 (Optional) Configure the retry interval.

Example:

```
Device(config-wireless-mesh-profile-fast-teardown)# interval duration
```

The valid range is from 1 to 10 seconds.

Step 6 (Optional) Set the latency interval so that at least one ping succeeds within your chosen threshold time.

Example:

```
Device(config-wireless-mesh-profile-fast-teardown)# latency-exceeded-threshold duration
```

The valid range is from 1 to 30 seconds.

Step 7 (Optional) Specify the latency threshold.

Example:

```
Device(config-wireless-mesh-profile-fast-teardown)# latency-threshold threshold-range
```

The valid range is from 1 to 500 milliseconds.

Step 8 (Optional) Specify the number of retries until the gateway is considered unreachable.

Example:

```
Device(config-wireless-mesh-profile-fast-teardown)# retries retry-limit
```

The valid range is from 1 to 10.

Step 9 (Optional) Specify the time during which root access point uplink has to be stable to accept child connections.

Example:

```
Device(config-wireless-mesh-profile-fast-teardown)# uplink-recovery-intervals recovery
interval
```

The valid range is from 1 to 3600 seconds.

You have configured the mesh AP profile with fast teardown enabled and applied custom parameters. This configuration improves your network's responsiveness to disruptions.

```
Device# configure terminal
Device(config)# wireless profile mesh mesh1
Device(config-wireless-mesh-profile)# fast-teardown
Device(config-wireless-mesh-profile-fast-teardown)# enabled
Device(config-wireless-mesh-profile-fast-teardown)# interval 5
Device(config-wireless-mesh-profile-fast-teardown)# latency-exceeded-threshold 20
Device(config-wireless-mesh-profile-fast-teardown)# latency-threshold 20
Device(config-wireless-mesh-profile-fast-teardown)# retries 1
Device(config-wireless-mesh-profile-fast-teardown)# uplink-recovery-intervals 1
```

Flex Resilient with Flex and Bridge Mode Access Points

Flex resilient with flex and bridge modes

A flex resilient system in flex and bridge modes is a network feature that

- operates within a configuration involving both flex and bridge mode APs
- allows the primary functionality of APs as mesh links between a root access point (RAP) and mesh access point (MAP), and
- ensures that the feature's operations are limited to flex and bridge mode APs.

Additional reference information

- Flex+Bridge Mode: A configuration mode combining the flexibility of standalone (local) management for APs with stable mesh network connectivity through root and mesh APs.
- Mesh Link Operation: Exists between RAP and MAP, allowing communication and bridging.
- Client Connectivity:
  - No new or disconnected clients can associate with a Mesh AP in flex+bridge mode.
  - Ongoing connections are maintained until a loss of the parent link for a child MAP.
- In a locally switching WLAN, the client traffic of a Flex+Bridge MAP is sent to the RAP's switchport.
- A child MAP that loses its parent connection cannot connect to a new parent without reacquiring a connection to the CAPWAP controller.

- The feature does not operate on non-Flex+Bridge mode APs.
- A new or disconnected wireless client cannot associate with a Mesh AP when in this mode.

Configure a flex profile (GUI)

Set up a flex profile to enhance network resilience and enable local authentication.

Use these steps to configure a flex profile using the GUI.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click a **Flex Profile Name**. The **Edit Flex Profile** dialog box appears.

Step 3 Under the **General** tab, choose the **Flex Resilient** check box to enable the Flex Resilient feature.

Step 4 Under the **VLAN** tab, choose the required VLANs.

Step 5 (Optionally) Under the **Local Authentication** tab, choose the desired server group from the **Local Accounting RADIUS Server Group** drop-down list. Also, choose the **RADIUS** check box.

Step 6 Click **Update & Apply to Device**.

The flex profile is successfully configured and updated in the system.

Configure a flex profile (CLI)

Configure a Flex Profile using commands on a network device to enable specific features and settings.

Use these steps to configure a flex profile using the CLI.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a flex profile and enters flex profile configuration mode using the **wireless profile flex** *flex-profile* command.

Example:

```
Device(config)# wireless profile flex new-flex-profile
```

Step 3 Enable ARP caching.

Example:

```
Device(config-wireless-flex-profile)# arp-caching
```

Step 4 Enable default parameters for the Flex profile using the **description** *description* command.

Example:

```
Device(config-wireless-flex-profile)# description "new flex profile"
```

Step 5 Configure native vlan-id information.

Example:

```
Device(config-wireless-flex-profile)# native-vlan-id 2660
```

Step 6 Enable the resilient feature.

Example:

```
Device(config-wireless-flex-profile)# resilient
```

Step 7 Configure VLAN name using the **vlan-name** *vlan_name* command.

Example:

```
Device(config-wireless-flex-profile)# vlan-name VLAN2659
```

Step 8 Configure the VLAN ID.

Example:

```
Device(config-wireless-flex-profile)# vlan-id 2659
```

The valid VLAN ID ranges from 1 to 4096.

Step 9 Exit the configuration mode and return to the privileged EXEC mode.

Example:

```
Device(config-wireless-flex-profile)# end
```

The Flex profile is configured on the network device with the specified settings and features.

Configure a site tag (CLI)

Configure a site tag on a network device to manage wireless networks efficiently and map APs to specific site tags.

Use these steps to configure a site tag using CLI.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a site tag and enter site tag configuration mode using the **wireless tag site** *site-name* command.

Example:

```
Device(config)# wireless tag site new-flex-site
```

Step 3 Configure a flex profile using the **flex-profile** *flex-profile-name* command.

Example:

```
Device(config-site-tag)# flex-profile new-flex-profile
```

Step 4 Remove **Local site** configured from the site tag.

Example:

```
Device(config-site-tag)# no local-site
```

Step 5 Map a site tag to an AP using the **site-tag** *site-tag-name* command.

Example:

```
Device(config-site-tag)# site-tag new-flex-site
```

Step 6 Exit configuration mode and return to privileged EXEC mode.

Example:

```
Device(config-site-tag)# end
```

The site tag is configured and mapped to the specified AP, facilitating effective management of wireless networks within the defined site tag.

Configure a mesh profile (CLI)

Configure a mesh profile on a network device to enable communication between mesh nodes, ensuring VLAN awareness and connectivity management.

Use these steps to configure a mesh profile using CLI commands.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a mesh profile and enter the mesh profile configuration mode using the **wireless profile mesh** *profile-name* command.

Example:

```
Device(config)# wireless profile mesh Mesh_Profile
```

Step 3 Disable VLAN transparency to ensure that the bridge is VLAN aware.

Example:

```
Device(config-wireless-profile-mesh)# no ethernet-vlan-transparent
```

Step 4 Exit the configuration mode and return to the privileged EXEC mode.

Example:

```
Device(config-wireless-profile-mesh)# end
```

The mesh profile is configured, VLAN transparency is disabled to ensure VLAN awareness, and the device returns to privileged EXEC mode.

Associate the wireless mesh to an AP profile (CLI)

Associate a wireless mesh to an AP profile to ensure proper configuration and management of AP.

Use these steps to associate the wireless mesh to an AP profile.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the AP profile and enter AP profile configuration mode using the **ap profile** *ap-profile-name* command.

Example:

```
Device(config)# ap profile new-ap-join-profile
```

Step 3 Configure the mesh profile in AP profile configuration mode using the **mesh-profile** *mesh-profile-name* command.

Example:

```
Device(config-ap-profile)# mesh-profile Mesh_Profile
```

Step 4 Configure the Secure Shell (SSH).

Example:

```
Device(config-ap-profile)# ssh
```

Step 5 Specify the AP management username and password for managing APs using the **mgmtuser username** *username* **password** {**0** | **8**} *password* command.

Example:

```
Device(config-ap-profile)# mgmtuser username Cisco password 0 Cisco secret 0 Cisco
```

- **0**: Specifies an UNENCRYPTED password.
- **8**: Specifies an AES encrypted password.

Note
While configuring a username, ensure that special characters are not used as they can lead to configuration errors.

Step 6 Exit configuration mode and return to privileged EXEC mode.

Example:

```
Device(config-ap-profile)# end
```

The AP profile is configured with the wireless mesh, allowing for proper management and operation of the AP.

Attach site tag to an access point (CLI)

Attach a site tag for AP identification and configuration management.

Use these steps to attach a site tag to an AP:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure APs and enters ap-tag configuration mode using the **ap** *mac-address* command.

Example:

```
Device(config)# ap F866.F267.7DFB
```

Step 3 Map a site tag to the AP using the**site-tag** *site-tag-name* command.

Example:

```
Device(config-ap-tag)# site-tag new-flex-site
```

Note
Associating Site Tag causes the associated AP to reconnect.

Step 4 Exit configuration mode and return to privileged EXEC mode.

Example:

```
Device(config-ap-tag)# end
```

The AP is now associated with the specified site tag and will reconnect.

Configure switch interface for APs (CLI)

Configure a switch interface for APs using CLI to ensure proper VLAN assignment and trunk settings.

Use these steps to configure switch interface for APs:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter the interface to be added to the VLAN.

Example:

```
Device(config)# interface <int-id>
```

Step 3 Assign the allowed VLAN ID to the port using the **switchport trunk native vlan** *vlan-id* command.

Example:

```
Device(config-if)# switchport trunk native vlan 2660
```

Step 4 Assign the allowed VLAN ID to the port using the **switchport trunk allowed vlan** *vlan-id* command.

Example:

```
Device(config-if)# switchport trunk allowed vlan 2659,2660
```

Step 5 Sets the trunking mode to trunk unconditionally.

Example:

```
Device(config-if)# switchport mode trunk
```

Note
When the controller works as a host for spanning tree, ensure that you configure portfast trunk, using **spanning-tree portfast trunk** command, in the uplink switch to ensure faster convergence.

Step 6 Exit configuration mode and return to privileged EXEC mode.

Example:

```
Device(config-if)# end
```

The switch interface is successfully configured for AP connectivity, enabling effective VLAN management and ensuring faster network convergence for connected APs.

Verify flex resilient with flex and bridge mode AP configuration

Use this command to view details about the AP mode and model.

```
Device# show ap name <ap-name> config general | inc AP Mode
AP Mode                                         : Flex+Bridge
AP Model                                        : AIR-CAP3702I-A-K9
```

Use this command to view the MAP mode details.

```
Device# show ap name MAP config general | inc AP Mode
AP Mode                                         : Flex+Bridge
AP Model                                        : AIR-CAP3702I-A-K9
```

Use this command to view the RAP mode details.

```
Device# show ap name RAP config general | inc AP Mode
AP Mode                                         : Flex+Bridge
AP Model                                        : AIR-AP2702I-A-K9
```

Use this command to check the status of the Flex Profile—Resilient feature.

```
Device# show  wireless profile flex detailed FLEX_TAG | inc resilient
Flex resilient                : ENABLED
```

Verify ATF configuration on mesh

You can verify Cisco ATF configurations on mesh APs using these commands.

Use this **show** command to display the ATF configuration summary of all the radios:

```
Device# show ap airtime-fairness summary

AP Name                           MAC Address       Slot Admin    Oper        Mode
  Optimization
---------------------------------- ----------------- ---- -------- ----------- --------------
 ------------
ap1/2                             6c:99:89:0c:73:a0 0    ENABLED  DOWN        Enforce-Policy
 Enabled
ap1/2                             6c:99:89:0c:73:a0 1    ENABLED  UP          Enforce-Policy
 Enabled
ap1/3                             6c:99:89:0c:73:a1 0    ENABLED  DOWN        Enforce-Policy
 Enabled
ap1/3                             6c:99:89:0c:73:a1 1    ENABLED  UP          Enforce-Policy
 Enabled
```

Use this **show** command to display the ATF configuration for a 2.4-GHz radio:

```
Device# show ap dot11 24ghz airtime-fairness

AP Name                           MAC Address       Slot Admin    Oper        Mode
  Optimization
------------------------------- ------------------   ---- -------- ----------- --------------
 ------------
ap1/2                             6c:99:89:0c:73:a0 1    ENABLED  UP          Enforce-Policy
 Enabled
```

Use this **show** command to display the ATF WLAN statistics:

```
Device# show ap name ap1 dot11 24ghz airtime-fairness wlan 12 statistics

AP Name                           MAC Address       Slot Admin    Oper        Mode
  Optimization
---------------------------------- ----------------- ---- -------- ----------- --------------
 ------------
ap1/2                             6c:99:89:0c:73:a0 0    ENABLED  DOWN        Enforce-Policy
 Enabled
ap1/2                             6c:99:89:0c:73:a0 1    ENABLED  UP          Enforce-Policy
 Enabled      Network level
```

Use this **show** command to display the wireless mesh summary:

```
Device# show wireless profile mesh summary

Number of Profiles: 2

Profile-Name                        BGN         Security  Bh-access  Description

------------------------------------------------------------------------------------------------
mesh1                                           EAP       DISABLED

default-mesh-profile                            EAP       DISABLED   default mesh profile
```

Use this **show** command to display the mesh ATF client access information:

```
Device# show mesh atf client-access

AP Name             Client Access Allocation   Override   Current nodes
                     Default %    Current %
```

```
------------------   ---------    ---------    --------   -------------
RAP                    25           40         Enabled          4
RAP                    33           40         Enabled          3
```

Verify mesh Ethernet daisy chaining

Use the **show ap config general** command to find out if a Persistent SSID is configured for an AP.

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

Persistent SSID Broadcast                    Enabled/Disabled
```

Use the **show wireless mesh persistent-ssid-broadcast summary** command to view the Persistent SSID broadcast status for all bridge root APs

```
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
```

Verify mesh convergence

This example shows the output from the **show wireless profile mesh detailed** command, which displays the mesh convergence method.

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

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

This example shows the output from **show wireless mesh convergence subset-channels** command, which displays the subset channels for the selected bridge group name.

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

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

Verify DHCP server for root AP configuration

To verify the DHCP server for root AP configuration, use this command:

```
Device# show ap config general
Cisco AP Name   : AP4C77.6DF2.D588
================================================
<SNIP>
Dhcp Server                                    : Enabled
```

Verify mesh backhaul

Use the **show ap name mesh backhaul** command to view 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
```

Use the **show wireless mesh ap backhaul** command to view 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
```

Use the **show ap summary** command to view 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
```

Verify mesh configuration

Use these **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 this **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 this **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 this **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 this **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 this **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 this **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 this **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 this **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 this **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 this **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 this **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 this **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 this **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 this **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 this **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 backhaul slot for root AP

Use this **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
```

Use a link test on mesh backhaul

Use this **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 this **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
```

Verify dot11ax rates on mesh backhaul

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

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

Verify mesh serial backhaul

To verify mesh AP serial backhaul, run this command:

```
Device# show ap name MAP-SB config slot 2 | inc Mesh
Mesh Radio Role : Downlink Access
Mesh Backhaul : Enabled
Mesh Designated Downlink : Enabled
```

To verify serial backhaul enabled on a specific AP, run this command:

```
Device# show ap name MAP-SB mesh backhaul
MAC Address : 4cxx.4dxx.f4xx
Current Backhaul Slot: 1
Radio Type: Main
Radio Subband: All
Mesh Radio Role: Uplink Access <<<<<<
Administrative State: Enabled
Operation State: Up
Current Tx Power Level: 6
Current Channel: (104) <<<<<<
Antenna Type:
Internal Antenna Gain (in .5 dBm units): 1
MAC Address : 4cxx.4dxx.f4xx
Current Backhaul Slot: 2
Radio Type: Slave
Radio Subband: All
Mesh Radio Role: Downlink Access <<<<<<
Administrative State: Enabled
Operation State: Up
Current Tx Power Level: 8
Current Channel: (149) <<<<<<
Antenna Type:
Internal Antenna Gain (in .5 dBm units): 1
```

To verify mesh serial backhaul, run this command:

```
Device# show wireless profile radio detailed radio-mesh-downlink
Radio Profile name                              : radio-mesh-downlink
Description                                     :
Beam-Selection                                  : Not configured
Number of antenna to be enabled                 : 0
Mesh Backhaul                                   : Enabled
Mesh Designated Downlink                        : Enabled
```

Verify the RRM DCA status

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

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

Note The output for the **show ap config general | i Mesh** and the **show ap name <AP name> config general | i Mesh** command displays only the status for manual RRM DCA triggers performed with the **ap name <AP name> dot11 rrm channel update mesh** command.

The output for the **show ap config general | i Mesh** and the **show ap name <AP name> config general | i Mesh** commands, does not update if only the global mesh RRM DCA is enabled (auto-DCA).

Verify fast teardown with default mesh profile

To verify the fast teardown with the default mesh profile, use this 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
```

Verify background scanning and MAP fast ancestor find

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

To verify the background scan, use this command:

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

To verify MAP Fast Ancestor Find, use this command:

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