Mesh Access Points

Introduction to the Mesh Network

Mesh networking employs Cisco Aironet outdoor mesh access points and indoor mesh access points along with Cisco Wireless Controller and Cisco Prime Infrastructure to provide scalability, central management, and mobility between indoor and outdoor deployments. Control and Provisioning of Wireless Access Points (CAPWAP) protocol manages the connection of mesh access points to the network.

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

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

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

Restrictions for Mesh Access Points

The Mesh feature is supported only on the following AP platforms:

- Outdoor APs
  - Cisco Industrial Wireless 3702 Access Points (supported from Cisco IOS XE Gibraltar 16.11.1b).
  - Cisco Aironet 1542 Access Points
  - Cisco Aironet 1562 Access Points
  - Cisco Aironet 1572 Access Points
  - Cisco Catalyst IW6300 Heavy Duty Access Points
  - Cisco 6300 Series Embedded Services Access Points
- Indoor APs
  - Cisco Aironet 1700 Access Points
  - Cisco Aironet 1800i Access Points
  - Cisco Aironet 1815i Access Points
  - Cisco Aironet 1815m Access Points
  - Cisco Aironet 1815w Access Points
  - Cisco Aironet 1832i Access Points

- Cisco Aironet 1852i Access Points
- Cisco Aironet 1852e Access Points
- Cisco Aironet 2700 Access Points
- Cisco Aironet 2802i Access Points
- Cisco Aironet 2802e Access Points
- Cisco Aironet 3700 Access Points
- Cisco Aironet 3802i Access Points
- Cisco Aironet 3802e Access Points
- Cisco Aironet 3802p Access Points
- Cisco Aironet 4800 Access Points

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.

MAC Authorization

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

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

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

Preshared Key Provisioning

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

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

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

EAP Authentication

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

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

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

EAP Authentication with LSC

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

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

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

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

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

Bridge Group Names

Bridge group names (BGNs) control the association of MAPs to the parent mesh AP. BGNs can logically group radios to avoid two networks on the same channel from communicating with each other. The setting is also useful if you have more than one RAP in your network in the same sector (area). BGN is a string comprising a maximum of 10 characters.

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

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

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

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

Preferred Parent Selection

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

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

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

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

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

Background Scanning

Mesh background scanning improves convergence time, and reliability and stability of parent selection. With the help of the Background Scanning feature, a MAP can find and connect with a better potential parent across channels, and maintain its uplink with the appropriate parent all the time.

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 AWPP link.

Mesh Backhaul at 2.4 GHz and 5 GHz

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

Mesh backhaul is supported at 2.4-GHz and 5-GHz. However, in certain countries it is not allowed to use mesh network with a 5-GHz backhaul network. The 2.4-GHz radio frequencies allow you to achieve much larger mesh or bridge distances. When a RAP gets a slot-change configuration, it gets propagated from the RAP to all its child MAPs. All the MAPs get disconnected and join the new configured backhaul slot.

Dynamic Frequency Selection

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

Country Codes

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

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

- Regulatory domain code

- Set of channels supported
- Transmit power level

Intrusion Detection System

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

Mesh Interoperability Between Controllers

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

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

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

Information About DHCP and NAT Functionality on Root AP (RAP)

Note This feature is applicable for Cisco Aironet 1542 series outdoor access points only.

The access points associated to a mesh network can play one of the two roles:

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

DHCP and NAT Functionality on Root AP - IPv4 Scenario

This feature enables the controller to send a TLV to RAP when a new RAP joins the controller.

The following covers the workflow:

- Controller pushes TLV to RAP for enabling DHCP and NAT functionality.
- Client associates to an SSID.
- RAP executes DHCP functionality to assign private IPv4 address to the client.
- RAP executes NAT functionality to get the private IPv4 address of the client and allow access to the network.

Mesh Convergence

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

The following convergence methods are supported.

Table 1: Mesh Convergence

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

Noise-Tolerant Fast

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

Ethernet Bridging

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

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

In a point-to-point bridging scenario, a Cisco Aironet 1500 Series MAP can be used to extend a remote network by using the backhaul radio to bridge multiple segments of a switched network. This is fundamentally a

wireless mesh network with one MAP and no WLAN clients. Just as in point-to-multipoint networks, client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access. To use an Ethernet-bridged application, enable the bridging feature on the RAP and on all the MAPs in that sector.

Ethernet bridging should be enabled for the following scenarios:

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

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

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

VLAN Tagging for MAP Ethernet Clients

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

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

Multicast Over Mesh Ethernet Bridging Network

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

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

The three mesh multicast modes are:

- Regular mode: Data is multicast across the entire mesh network and all its segments by bridging-enabled RAP and MAP.
- In-only mode: Multicast packets received from the Ethernet by a MAP are forwarded to the corresponding RAP's Ethernet network. No additional forwarding occurs, which ensures that non-CAPWAP multicasts received by the RAP are not sent back to the MAP Ethernet networks within the mesh network (their point of origin), and MAP to MAP multicasts do not occur because such multicasts are filtered out.
- In-out mode: The RAP and MAP both multicast but in a different manner.

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

Radio Resource Management on Mesh

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

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

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

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

The Spectrum Intelligence feature scans for non-Wi-Fi radio interference on 2.4-GHz and 5-GHz bands. The feature supports client serving mode and monitor mode. The Cisco CleanAir technology in mesh backhaul and access radios provides an Interference Device Report (IDR) and Air Quality Index (AQI). Two key mitigation features (Event-Driven Radio Resource Management [EDRRM] and Persistence Device Avoidance [PDA]) are present in CleanAir. Both rely directly on information that can only be gathered by CleanAir. In the client-access radio band, they work the same way in mesh networks as they do in non-mesh networks in the backhaul radio band, the CleanAir reports are only displayed on the controller. No action is taken through ED-RRM.

Note that no specific configuration options are available to enable or disable CleanAir for MAPs.

For more information about Spectrum Intelligence, see #unique_1449 section.

Indoor Mesh Interoperability with Outdoor Mesh

Interoperability of indoor MAPs with outdoor APs are supported. This helps to bring coverage from outdoors to indoors. However, we recommend that you use indoor MAPs for indoor use only, and deploy them outdoors only under limited circumstances such as a simple short-haul extension from an indoor WLAN to a hop in a parking lot.

Mobility groups can be shared between outdoor mesh networks and indoor WLAN networks. It is also possible for a single controller to control indoor and outdoor MAPs simultaneously. Not that the same WLANs are broadcast out of both indoor and outdoor MAPs.

Workgroup Bridge

A workgroup bridge (WGB) is used to connect wired networks over a single wireless segment by informing the corresponding MAP of all the clients that the WGB has on its wired segment via IAPP messages. In addition to the IAPP control messages, the data packets for WGB clients contain an extra MAC address in the 802.11 header (four MAC headers, versus the normal three MAC data headers). 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.

APs can be configured as workgroup bridges. Only one radio interface is used for controller connectivity, Ethernet interface for wired client connectivity, and other radio interface for wireless client connectivity.

In Cisco Catalyst 9800 Series Wireless Controller, WGB acts as a client association, with the wired clients behind WGB supported for data traffic over the mesh network. Wired clients with different VLANs behind WGB are also supported.

Link Test

A link test is used to determine the quality of the radio link between two devices. Two types of link-test packets are transmitted during a link test: request and response. Any radio receiving a link-test request packet fills in the appropriate text boxes and 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 due to the asymmetrical distribution of the transmit power and receive sensitivity on both sides. Two types of link tests can be performed: a ping test and a CCX link test.

With the ping link test, the controller can test link quality only in the client-to-access point direction. The RF parameters of the ping reply packets received by the access point are polled by the controller to determine the client-to-access point link quality.

With the CCX link test, the controller can also test the link quality in the access point-to-client direction. The controller issues link-test requests to the client, and the client records the RF parameters (received signal strength indicator [RSSI], signal-to-noise ratio [SNR], and so on). of the received request packet in the response packet. Both the link-test requestor and responder roles are implemented on the access point and controller. Not only can the access point or controller initiate a link test to a CCX v4 or v5 client, but a CCX v4 or v5 client can initiate a link test to the access point or controller.

Mesh Daisy Chaining

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

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

The following are the guidelines for the daisy chaining mode:

- Primary MAP should be configured as mesh AP.
- Subordinate MAP should be configured as root AP.
- Daisy chaining should be enabled on both primary and subordinate MAP.
- Ethernet bridging should be enabled on all the APs in the Bridge mode. Enable Ethernet bridging in the mesh profile and map all the bridge mode APs in the sector to the same mesh profile.

- VLAN support should be enabled on the wired root AP, subordinate MAP, and primary MAP along with proper native VLAN configuration.

Mesh Leaf Node

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

Flex+Bridge Mode

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

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

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

- FlexConnect
- Flex+Bridge (FlexConnect+Mesh)

Backhaul Client Access

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

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

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

Mesh CAC

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

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

Mesh CAC is not supported for the following scenarios.

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

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

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

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

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

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

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

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

Configuring MAC Authorization (GUI)

Procedure

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

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

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

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

Both WebUI and CLI support mac user configuration in one of these formats: xxxxxxxxxxxx, xx:xx:xx:xx:xx:xx, xx-xx-xx-xx-xx-xx, or xxxx.xxxx.xxxx where AP sends the default mac address without delimiter. If the mac address is configured with delimiter, then AP authorization will fail unless it is configured in the format: xxxxxxxxxxxx.

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

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

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

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

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

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

Step 9 Click the **Advanced** tab.

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

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

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

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

Configuring MAC Authorization (CLI)

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

Before you begin

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

Procedure

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

Configuring MAP Authorization - EAP (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.

dot1x

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** window 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**.

Configuring MAP Authorization (CLI)

Select and configure authentication method of EAP/PSK for MAP authentication.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa authentication** *method-name* **radius group** *server-group-name* **Example:** `Device(config)# aaa authentication dot1x auth1 radius group radius-server-1`	For local authentication: `Device(config)# aaa authentication dot1x auth1 local` Sets an authentication method list to use a RADIUS server group. This is required for EAP authentication.
Step 3	**wireless profile mesh** *profile--name* **local** **Example:**	Sets an authorization method list to use local credentials.

	Command or Action	Purpose
	`Device(config)# wireless profile mesh mesh1`	
Step 4	**security eap** *server-group-name* **Example:** `Device(config-wireless-mesh-profile)# security eap / psk`	Configures the mesh security EAP/PSK for mesh AP.
Step 5	**method authentication** *method-name* **Example:** `Device(config-wireless-mesh-profile)# method authentication auth1`	Configures the authentication method for mesh AP authentication.

Configuring PSK Provisioning (CLI)

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

Follow the procedure given below to configure a PSK:

Before you begin

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

Note

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh security psk provisioning** **Example:** `Device(config)# wireless mesh security psk provisioning`	Configures the security method for wireless as PSK. **Note** The provisioned PSK is pushed only to those APs that are configured with PSK as the mesh security method.

	Command or Action	Purpose
Step 3	**wireless mesh security psk provisioning key** *index* {**0** | **8**} *pre-shared-key description* **Example:** `Device(config)# wireless mesh security psk provisioning key 1 0 secret secret-key`	Configures a new PSK for mesh APs.
Step 4	**wireless mesh security psk provisioning default-psk** **Example:** `Device(config)# wireless mesh security psk provisioning default-psk`	Enables default PSK-based authentication.
Step 5	**wireless mesh security psk provisioning inuse** *index* **Example:** `Device(config)# wireless mesh security psk provisioning inuse 1`	Specifies the PSK to be actively used. **Note** You should explicitly set the in-use key index in the global configuration pointing to the PSK index.

Configuring a Bridge Group Name (GUI)

Procedure

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

Step 2 Click **Add**.

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

Step 4 Click **Apply to Device**.

Configuring a Bridge Group Name (CLI)

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

Procedure

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

Configuring Background Scanning (GUI)

Procedure

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

Step 2 Choose a profile.

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

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

Configuring Background Scanning

Procedure

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

	Command or Action	Purpose
Step 3	**background-scanning** **Example:** `Device(config-wireless-mesh-profile)# background-scanning`	Configures background scanning in mesh deployments.

Configuring Backhaul Client Access (GUI)

Procedure

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

Step 2 Choose a profile.

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

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

Configuring Backhaul Client Access (CLI)

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

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

Procedure

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

Configuring Wireless Backhaul Data Rate (CLI)

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

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

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

Procedure

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

Configuring Dynamic Frequency Selection (CLI)

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

Procedure

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

Configuring the Intrusion Detection System (CLI)

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**ids** **Example:** `Device(config-wireless-mesh-profile)# ids`	Configures intrusion detection system reporting for mesh APs.

Configuring Ethernet Bridging (GUI)

Procedure

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

Step 2 Click **Add**.

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

Step 4 In **Advanced** tab, check the **Ethernet Bridging** check box.

Step 5 Click **Apply to Device**.

Configuring Ethernet Bridging (CLI)

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

Ethernet bridging can be enabled for the following scenarios:

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

Before you begin

- Ensure that you configure the following commands under the mesh profile configuration for Ethernet bridging to be enabled:
  - **ethernet-bridging**: Enables the Ethernet Bridging feature on an AP.
  - **no ethernet-vlan-transparent**: Makes the wireless mesh bridge VLAN aware. Allows VLAN filtering with the following AP command: **[no] mesh ethernet** {**0** | **1** | **2** | **3**} **mode trunk vlan allowed**.

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

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

- For FlexConnect+Brigde APs, configure the native VLAN ID under the corresponding flex profile.

Procedure

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

Configuring Multicast Modes over Mesh

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

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

Configuring RRM on Mesh Backhaul (CLI)

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

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

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

Procedure

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

Selecting a Preferred Parent (GUI)

Procedure

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

Step 2 Click the Access Point.

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

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

Selecting a Preferred Parent (CLI)

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

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

Procedure

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

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

Changing the Role of an AP (GUI)

Procedure

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

Step 2 Click the **Access Point**.

Step 3 In the **Mesh** tab, choose **Root** or **Mesh** from the **Role** drop-down list.

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

After the role change is triggered, the AP reboots.

Changing the Role of an AP (CLI)

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

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

Procedure

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

Configuring the Mesh Leaf Node (CLI)

Procedure

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

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

Configuring the Mesh Leaf Node (GUI)

Procedure

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

Step 2 Click the Access Point.

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

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

Configuring Subset Channel Synchronization

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

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

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

Procedure

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

Provisioning LSC for Bridge-Mode and Mesh APs (GUI)

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 using the MAC address and add them. The APs added to the provision list are displayed 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**.

Provisioning LSC for Bridge-Mode and Mesh APs

- Configuring Locally Significant Certificate (LSC) will not remove pre-existing certificates from an AP.
- An AP can have both LSC and Message Integrity Check (MIC) certificates. However, when an AP is provisioned with LSC, the MIC certificate is not used on boot-up. A change from LSC to MIC requires the AP to reboot.

Follow the procedure given below to configure LSC for bridge-mode and mesh APs:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision** **Example:** `Device(config)# ap lsc-provision`	Configures LSC provisioning on an AP. **Note** This step is applicable only for mesh APs.
Step 3	**ap lsc-provision provision-list** **Example:**	(Optional) Configures LSC provision for all the APs in the provision list.

	Command or Action	Purpose
	`Device(config)# ap lsc-provision provision-list`	
Step 4	**aaa authentication dot1x** *auth-list* **radius group** *radius-server-grp* **Example:** `Device(config)# aaa authentication dot1x list1 radius group sg1`	Configures named authorization list for downloading EAP credential from radius group server.
Step 5	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 6	**lsc-only-auth** **Example:** `Device(config-wireless-mesh-profile)# lsc-only-auth`	Configures mesh security to LSC-only MAP authentication. After this command is run, all the mesh APs reboot.
Step 7	**method authorization** *local* **Example:** `Device(config-wireless-mesh-profile)# method authorization list1`	Configures an authorization method for mesh AP authorization.

Specifying the Backhaul Slot for the Root AP (GUI)

Procedure

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

Step 2 Click **Add**.

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

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

Step 5 Click **Apply to Device**.

Specifying the Backhaul Slot for the Root AP (CLI)

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

Procedure

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

Using a Link Test on Mesh Backhaul (GUI)

Procedure

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

Step 2 Click the Access Point.

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

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

Step 5 Click **Start**.

Using a Link Test on Mesh Backhaul

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

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

Procedure

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

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

Configuring Battery State for Mesh AP (GUI)

Procedure

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

Step 2 Choose a profile.

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

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

Configuring Battery State for Mesh AP

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

Procedure

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

Configuring DHCP Server on Root Access Point (RAP)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures an AP Profile.
Step 3	**dhcp-server** **Example:** `Device(config-ap-profile)# dhcp-server`	Configures DHCP server on the root access point.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Saves the configuration and exits configuration mode and returns to privileged **EXEC** mode.

Configuring Mesh CAC (CLI)

Procedure

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

Configuring ATF on Mesh (GUI)

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 choose the **Mode**, click the **Monitor** or **Enforced** radio button.

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

Step 5 Enter the **Airtime Allocation**.

Step 6 Click **Apply to Device**.

Configuring ATF on Mesh

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rf-profile** *rf-profile* **Example:** `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	Configures an RF profile and enters RF profile configuration mode.
Step 3	**airtime-fairness bridge-client-access airtime-allocation** *allocation-weight-percentage* **Example:** `Device(config-rf-profile)# airtime-fairness bridge-client-access airtime-allocation 10`	Configures airtime allocation weight percentage on mesh APs.

Create an ATF Policy for a MAP

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**dot11 24ghz airtime-fairness** *atf-policy* **Example:** `Device(config-wireless-policy)# dot11 24ghz airtime-fairness atf-policy`	Enables ATF in the existing RF profile.

Creating an ATF Policy (GUI)

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 Weighted ratio is used instead of percentages so that the total can 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.

Adding an ATF to a Policy Profile (GUI)

Procedure

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

Step 2 Click the name of the corresponding policy profile.

Step 3 Click the **Advanced** tab.

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

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

Enabling ATF Mode in an RF Profile (GUI)

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 for the following:

- **Status**—If you choose **Enabled** as the status, select the **Mode** as either **Monitor** or **Enforced**. Also, you can 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**.

Configuring Fast Teardown for a Mesh AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters the mesh profile configuration mode.
Step 3	**fast-teardown** **Example:** `Device(config-wireless-mesh-profile)# fast-teardown`	Enables the fast teardown of mesh network and configures the feature's parameter.
Step 4	**enabled** **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# enabled`	Enables the fast teardown feature.
Step 5	**interval** *duration* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# interval 5`	(Optional) Configures the retry interval. The valid values range between 1 and 10 seconds.
Step 6	**latency-exceeded-threshold** *duration* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# latency-exceeded-threshold 20`	(Optional) Specifies the latency interval at which at least one ping must succeed in less than threshold time. The valid values range between 1 and 30 seconds.
Step 7	**latency-threshold** *threshold range* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# latency-threshold 20`	(Optional) Specifies the latency threshold. The valid values range between 1 and 500 milliseconds.
Step 8	**retries** *retry limit* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# retries 1`	(Optional) Specifies the number of retries until the gateway is considered unreachable. The valid values range between 1 and 10.
Step 9	**uplink-recovery-intervals** *recovery interval* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# uplink-recovery-intervals 1`	(Optional) Specifies the time during which root access point uplink has to be stable to accept child connections. The valid values range between 1 and 3600 seconds.

Verifying ATF Configuration on Mesh

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

Use the following **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 the following **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 the following **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 the following **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
```

```
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
```

Verifying DHCP Server for Root AP Configuration

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

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

Verifying Mesh Configuration

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

- **show wireless mesh stats** *ap-name*
- **show wireless mesh security-stats** {*all* | *ap-name*}
- **show wireless mesh queue-stats** {*all* | *ap-name*}
- **show wireless mesh per-stats summary** {*all* | *ap-name*}
- **show wireless mesh neighbor summary** {*all* | *ap-name*}
- **show wireless mesh neighbor detail** *ap-name*
- **show wireless mesh ap summary**
- **show wireless mesh ap tree**
- **show wireless mesh ap backhaul**
- **show wireless mesh config**
- **show wireless mesh convergence detail** *bridge-group-name*
- **show wireless mesh convergence subset-channels**
- **show wireless mesh neighbor**
- **show wireless profile mesh detailed** *mesh-profile-name*
- **show wireless stats mesh security**
- **show wireless stats mesh queue**
- **show wireless stats mesh packet error**
- **show wireless mesh ap summary**
- **show ap name** *ap-name* **mesh backhaul**
- **show ap name** *ap-name* **mesh neighbor detail**
- **show ap name** *ap-name* **mesh path**
- **show ap name** *ap-name* **mesh stats packet error**
- **show ap name** *ap-name* **mesh stats queue**
- **show ap name** *ap-name* **mesh stats security**
- **show ap name** *ap-name* **mesh stats**

- **show ap name** *ap-name* **mesh bhrate**
- **show ap name** *ap-name* **config ethernet**
- **show ap name** *ap-name* **cablemodem**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **gps location**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **mesh linktest data** *dest-mac*
- **show ap environment**
- **show ap gps location**

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

MAC Authorization

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

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

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

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

PSK Provisioning

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

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

Mesh Alarm Criteria
  Max Hop Count                                 :  4
  Recommended Max Children for MAP              : 10
  Recommended Max Children for RAP              : 20
```

```
  Low Link SNR                                    : 12
  High Link SNR                                   : 60
  Max Association Number                          : 10
  Parent Change Number                            :  3

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

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

Bridge Group Name

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

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
Multicast Mode                : In-Out
Range in feet                 : 12000
Security Mode                 : EAP
Convergence Method            : Fast
LSC only Authentication       : DISABLED
Battery State                 : ENABLED
Authorization Method          : CENTRAL_AUTHOR
Authentication Method         : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

Backhaul Client Access

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

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

Wireless Backhaul Data Rate

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

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

Dynamic Frequency Selection

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

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

Intrusion Detection System

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

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

Ethernet Bridging

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

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

Multicast over Mesh

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

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

RRM on Mesh Backhaul

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

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

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

Mesh PSK Config
  PSK Provisioning                              : ENABLED
```

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

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

Preferred Parent Selection

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

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

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

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

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

AP Role Change

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

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

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

Mesh Leaf Node

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

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

Cisco AP Identifier                              : 7070.8bbc.d3e0
Country Code                                     : Multiple Countries : IN,US,IO,J4
Regulatory Domain Allowed by Country             : 802.11bg:-AEJPQU   802.11a:-ABDJNPQU
AP Country Code                                  : IN  - India
AP Regulatory Domain
  Slot 0                                         : -A
  Slot 1                                         : -D
MAC Address                                      : 500f.8095.01e4
...
```

```
AP Mode                                          : Bridge
Mesh profile name                                : abc-mesh-profile
AP Role                                          : Mesh AP
Backhaul radio type                              : 802.11a
Backhaul slot id                                 : 1
Backhaul tx rate                                 : auto
Ethernet Bridging                                : Enabled
Daisy Chaining                                   : Disabled
Strict Daisy Rap                                 : Disabled
Bridge Group Name                                : bgn-abc
Strict-Matching BGN                              : Enabled
Preferred Parent Address                         : 7070.8b7a.6fb8
Block child state                                : Disabled
PSK Key Timestamp                                : Not Configured
...
FIPS status                                      : Disabled
WLANCC status                                    : Disabled
GAS rate limit Admin status                      : Disabled
WPA3 Capability                                  : Disabled
EWC-AP Capability                                 : Disabled
AWIPS Capability                                 : Disabled
Proxy Hostname                                   : Not Configured
Proxy Port                                       : Not Configured
Proxy NO_PROXY list                              : Not Configured
GRPC server status                               : Disabled
```

Subset Channel Synchronization

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

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

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

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

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

Provisioning LSC for Bridge-Mode and Mesh APs

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

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name             : default-mesh-profile
```

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

Specify the Backhaul Slot for the Root AP

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

```
Device# show ap name 1542-RAP mesh backhaul
MAC Address : 380e.4d85.5e60
  Current Backhaul Slot: 1
  Radio Type: 0
  Radio Subband: All
  Mesh Radio Role: DOWNLINK
  Administrative State: Enabled
  Operation State: Up
  Current Tx Power Level:
  Current Channel: (165)
  Antenna Type: N/A
  Internal Antenna Gain (in .5 dBm units): 18
```

Using a Link Test on Mesh Backhaul

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

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

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

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

Mesh CAC

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

```
Device# show wireless mesh config
Mesh Config
```

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

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

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

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