



Mesh Access Point Commands

- [config mesh alarm, on page 3](#)
- [config mesh astools, on page 4](#)
- [config mesh backhaul rate-adapt, on page 5](#)
- [config mesh backhaul slot, on page 6](#)
- [config mesh battery-state, on page 7](#)
- [config mesh client-access, on page 8](#)
- [config mesh ethernet-bridging allow-bpdu, on page 9](#)
- [config mesh ethernet-bridging vlan-transparent, on page 10](#)
- [config mesh full-sector-dfs, on page 11](#)
- [config mesh linkdata, on page 12](#)
- [config mesh linktest, on page 14](#)
- [config mesh lsc, on page 17](#)
- [config mesh lsc advanced, on page 18](#)
- [config mesh lsc advanced ap-provision, on page 19](#)
- [config mesh multicast, on page 20](#)
- [config mesh parent preferred, on page 22](#)
- [config mesh public-safety, on page 23](#)
- [config mesh radius-server, on page 24](#)
- [config mesh range, on page 25](#)
- [config mesh secondary-backhaul, on page 26](#)
- [config mesh security, on page 27](#)
- [config mesh slot-bias, on page 29](#)
- [debug mesh security, on page 30](#)
- [show mesh ap, on page 31](#)
- [show mesh astools stats, on page 33](#)
- [show mesh backhaul, on page 34](#)
- [show mesh cac, on page 35](#)
- [show mesh client-access, on page 37](#)
- [show mesh config, on page 38](#)
- [show mesh env, on page 39](#)
- [show mesh neigh, on page 40](#)
- [show mesh path, on page 43](#)
- [show mesh per-stats, on page 44](#)

- [show mesh public-safety](#), on page 45
- [show mesh queue-stats](#), on page 46
- [show mesh security-stats](#), on page 47
- [show mesh stats](#), on page 49

config mesh alarm

To configure alarm settings for outdoor mesh access points, use the **config mesh alarm** command.

```
config mesh alarm { max-hop | max-children | low-snr | high-snr | association | parent-change count } value
```

Syntax Description		
max-hop		Sets the maximum number of hops before triggering an alarm for traffic over the mesh network. The valid values are 1 to 16 (inclusive).
max-children		Sets the maximum number of mesh access points (MAPs) that can be assigned to a mesh router access point (RAP) before triggering an alarm. The valid values are 1 to 16 (inclusive).
low-snr		Sets the low-end signal-to-noise ratio (SNR) value before triggering an alarm. The valid values are 1 to 30 (inclusive).
high-snr		Sets the high-end SNR value before triggering an alarm. The valid values are 1 to 30 (inclusive).
association		Sets the mesh alarm association count value before triggering an alarm. The valid values are 1 to 30 (inclusive).
parent-change count		Sets the number of times a MAP can change its RAP association before triggering an alarm. The valid values are 1 to 30 (inclusive).
<i>value</i>		Value above or below which an alarm is generated. The valid values vary for each command.

Command Default See the “Syntax Description” section for command and argument value ranges.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the maximum hops threshold to 8:

```
(Cisco Controller) >config mesh alarm max-hop 8
```

The following example shows how to set the upper SNR threshold to 25:

```
(Cisco Controller) >config mesh alarm high-snr 25
```

config mesh astools

To globally enable or disable the anti-stranding feature for outdoor mesh access points, use the **config mesh astools** command.

config mesh astools {enable | disable}

Syntax Description	enable	enable
	enable	Enables this feature for all outdoor mesh access points.
	disable	Disables this feature for all outdoor mesh access points.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable anti-stranding on all outdoor mesh access points:

```
(Cisco Controller) >config mesh astools enable
```

config mesh backhaul rate-adapt

To globally configure the backhaul Tx rate adaptation (universal access) settings for indoor and outdoor mesh access points, use the **config mesh backhaul rate-adapt** command.

config mesh backhaul rate-adapt [**all** | **bronze** | **silver** | **gold** | **platinum**] {**enable** | **disable**}

Syntax Description		
	all	(Optional) Grants universal access privileges on mesh access points.
	bronze	(Optional) Grants background-level client access privileges on mesh access points.
	silver	(Optional) Grants best effort-level client access privileges on mesh access points.
	gold	(Optional) Grants video-level client access privileges on mesh access points.
	platinum	(Optional) Grants voice-level client access privileges on mesh access points.
	enable	Enables this backhaul access level for mesh access points.
	disable	Disables this backhaul access level for mesh access points.

Command Default Backhaul access level for mesh access points is disabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines To use this command, mesh backhaul with client access must be enabled by using the **config mesh client-access** command.



Note After this feature is enabled, all mesh access points reboot.

The following example shows how to set the backhaul client access to the best-effort level:

```
(Cisco Controller) >config mesh backhaul rate-adapt silver
```

config mesh backhaul slot

To configure the slot radio as a downlink backhaul, use the **config mesh backhaul slot** command.

```
config mesh backhaul slot slot_id {enable | disable} cisco_ap
```

Syntax Description		
<i>slot_id</i>		Slot number between 0 and 2.
enable		Enables the entered slot radio as a downlink backhaul.
disable		Disables the entered slot radio as a downlink backhaul.
<i>cisco_ap</i>		Name of the Root AP of the sector on which the backhaul needs to be enabled or disabled.

Command Default The entered slot radio as a downlink backhaul is disabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines For 2.4 GHz, only slot 0 and 1 are valid. If slot 0 is enabled, slot 1 is automatically be disabled. If slot 0 is disabled, slot 1 is automatically enabled.

The following example shows how to enable slot 1 as the preferred backhaul for the root AP myrootap1:

```
(Cisco Controller) >config mesh backhaul slot 1 enable myrootap1
```

config mesh battery-state

To configure the battery state for Cisco mesh access points, use the **config mesh battery-state** command.

```
config mesh battery-state disable {all | cisco_ap}
```

Syntax	Description
disable	Disables the battery-state for mesh access points.
all	Applies this command to all mesh access points.
<i>cisco_ap</i>	Specific mesh access point.

Command Default Battery state is disabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable battery state for all mesh APs:

```
(Cisco Controller) >config mesh battery-state disable all
```

config mesh client-access

To enable or disable client access to the mesh backhaul on indoor and outdoor mesh access points, use the **config mesh client-access** command.

config mesh client-access { **enable** [**extended**] | **disable** }

Syntax Description	enable	extended	disable
	Allows wireless client association over the mesh access point backhaul 802.11a radio.	(Optional) Enables client access over both the backhaul radios for backhaul access points.	Restricts the 802.11a radio to backhaul traffic, and allows client association only over the 802.11b/g radio.

Command Default Client access is disabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines Backhaul interfaces (802.11a radios) act as primary Ethernet interfaces. Backhauls function as trunks in the network and carry all VLAN traffic between the wireless and wired network. No configuration of primary Ethernet interfaces is required.

When this feature is enabled, the mesh access points allow wireless client association over the 802.11a radio, which implies that a 152x mesh access point can carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio.

When this feature is disabled, the mesh access points carry backhaul traffic over the 802.11a radio and allows client association only over the 802.11b/g radio.

The following example shows how to enable client access extended to allow a wireless client association over the 802.11a radio:

```
(Cisco Controller) >config mesh client-access enable extended
Enabling client access on both backhaul slots
Same BSSIDs will be used on both slots
All Mesh AP will be rebooted
Are you sure you want to start? (y/N)Y
```

The following example shows how to restrict a wireless client association to the 802.11b/g radio:

```
(Cisco Controller) >config mesh client-access disable
All Mesh AP will be rebooted
Are you sure you want to start? (Y/N) Y
Backhaul with client access is canceled.
```


config mesh ethernet-bridging allow-bpdu

To configure STP BPDUs towards wired mesh uplink, use the **config mesh ethernet-bridging allow-bpdu** command.

```
config mesh ethernet-bridging allow-bpdu {enable | disable}
```

Syntax Description	enable	Enables STP BPDUs towards wired mesh uplink.
	disable	Disables STP BPDUs towards wired mesh uplink.
Command Default	Disabled	
Command History	Release	Modification
	8.0.110.0	This command was introduced.
Usage Guidelines	Cisco WLC does not allow you to use this command if VLAN transparency is enabled.	

config mesh ethernet-bridging vlan-transparent

To configure how a mesh access point handles VLAN tags for Ethernet bridged traffic, use the **config mesh ethernet-bridging vlan-transparent** command.

config mesh ethernet-bridging vlan-transparent { **enable** | **disable** }

Syntax Description	enable	Bridges packets as if they are untagged.
	disable	Drops all tagged packets.
Command Default	Bridges packets as if they are untagged.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure Ethernet packets as untagged:

```
(Cisco Controller) >config mesh ethernet-bridging vlan-transparent enable
```

The following example shows how to drop tagged Ethernet packets:

```
(Cisco Controller) >config mesh ethernet-bridging vlan-transparent disable
```

config mesh full-sector-dfs

To globally enable or disable full-sector Dynamic Frequency Selection (DFS) on mesh access points, use the `config mesh full-sector-dfs` command.

```
config mesh full-sector-dfs {enable | disable}
```

Syntax Description	enable	Enables DFS for mesh access points.
	disable	Disables DFS for mesh access points.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines This command instructs the mesh sector to make a coordinated channel change on the detection of a radar signal. For example, if a mesh access point (MAP) detects a radar signal, the MAP will notify the root access point (RAP), and the RAP will initiate a sector change.

All MAPs and the RAP that belong to that sector go to a new channel, which lowers the probability of MAPs stranding when radar is detected on the current backhaul channel, and no other valid parent is available as backup.

Each sector change causes the network to be silent for 60 seconds (as dictated by the DFS standard).

It is expected that after a half hour, the RAP will go back to the previously configured channel, which means that if radar is frequently observed on a RAP's channel, it is important that you configure a different channel for that RAP to exclude the radar affected channel at the controller.

This example shows to enable full-sector DFS on mesh access points:

```
(Cisco Controller) >config mesh full-sector-dfs enable
```



```

rx lost packets:      0 (incr for each pkt seq missed or out of order)
rx dup pkts:         0
rx out of order:     0
avgSNR:      30, high: 33, low: 3
SNR profile   [0dB...60dB]
    0          6          0          0          0
    0          0          1          2          77
    2888       3          0          0          0
    0          0          0          0          0
(>60dB)       0
avgNf:      -95, high: -67, low: -97
Noise Floor profile [-100dB...-40dB]
    0          2948       19          3          1
    0          0          0          0          0
    3          3          0          0          0
    0          0          0          0          0
(>-40dB)      0
avgRssi:     64, high: 68, low: 63
RSSI profile  [-100dB...-40dB]
    0          0          0          0          0
    0          0          0          0          0
    0          0          0          0          0
    0          0          0          0          0
(>-40dB)     2977
Summary PktFailedRate (Total pkts sent/recvd):          0.000%
Physical layer Error rate (Total pkts with errors/Total pkts heard): 0.000%

```

This example shows how to enable external MAC filtering on access point AP001d.71d.e300:

```

(Cisco Controller) >config mesh linkdata AP001d.710d.e300
[SD:0,0,0(0,0,0), 0,0, 0,0]
[SD:1,105,0(0,0,0), 30,704,95,707]
[SD:2,103,0(0,0,0), 30,46,95,25]
[SD:3,105,0(0,0,0), 30,73,95,29]
[SD:4,82,0(0,0,0), 30,39,95,24]
[SD:5,82,0(0,0,0), 30,60,95,26]
[SD:6,105,0(0,0,0), 30,47,95,23]
[SD:7,103,0(0,0,0), 30,51,95,24]
[SD:8,105,0(0,0,0), 30,55,95,24]
[SD:9,103,0(0,0,0), 30,740,95,749]
[SD:10,105,0(0,0,0), 30,39,95,20]
[SD:11,104,0(0,0,0), 30,58,95,23]
[SD:12,105,0(0,0,0), 30,53,95,24]
[SD:13,103,0(0,0,0), 30,64,95,43]
[SD:14,105,0(0,0,0), 30,54,95,27]
[SD:15,103,0(0,0,0), 31,51,95,24]
[SD:16,105,0(0,0,0), 30,59,95,23]
[SD:17,104,0(0,0,0), 30,53,95,25]
[SD:18,105,0(0,0,0), 30,773,95,777]
[SD:19,103,0(0,0,0), 30,745,95,736]
[SD:20,105,0(0,0,0), 30,64,95,54]
[SD:21,103,0(0,0,0), 30,747,95,751]
[SD:22,105,0(0,0,0), 30,55,95,25]
[SD:23,104,0(0,0,0), 30,52,95,35]
[SD:24,105,0(0,0,0), 30,134,95,23]
[SD:25,103,0(0,0,0), 30,110,95,76]
[SD:26,105,0(0,0,0), 30,791,95,788]
[SD:27,103,0(0,0,0), 30,53,95,23]
[SD:28,105,0(0,0,0), 30,128,95,25]
[SD:29,104,0(0,0,0), 30,49,95,24]
[SD:30,0,0,0(0,0,0), 0,0, 0,0]

```

config mesh linktest

To verify client access between mesh access points, use the **config mesh linktest** command.

config mesh linktest *source_ap* {*dest_ap* | *MAC addr*} *datarate* *packet_rate* *packet_size* *duration*

Syntax Description

<i>source_ap</i>	Source access point.
<i>dest_ap</i>	Destination access point.
<i>MAC addr</i>	MAC address.
<i>datarate</i>	<ul style="list-style-type: none"> • Data rate for 802.11a radios. Valid values are 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps. • Data rate for 802.11b radios. Valid values are 6, 12, 18, 24, 36, 54, or 100 Mbps. • Data rate for 802.11n radios. Valid values are MCS rates between m0 to m15.
<i>packet_rate</i>	Number of packets per second. Valid range is 1 through 3000, but the recommended default is 100.
<i>packet_size</i>	(Optional) Packet size in bytes. If not specified, packet size defaults to 1500 bytes.
<i>duration</i>	(Optional) Duration of the test in seconds. Valid values are 10-300 seconds, inclusive. If not specified, duration defaults to 30 seconds.

Command Default

100 packets per second, 1500 bytes, 30-second duration.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The **config mesh linktest** and **config mesh linkdata** commands are designed to be used together to verify information between a source and a destination access point. To get this information, first enter the **config mesh linktest** command with the access point that you want link data from in the *dest_ap* argument. When the command completes, enter the **config mesh linkdata** command and list the same destination access point, to display the link data.

The following warning message appears when you run a linktest that might oversubscribe the link:

```
Warning! Data Rate (100 Mbps) is not enough to perform this link test on
packet size (2000bytes) and (1000) packets per second. This may cause AP
to disconnect or reboot. Are you sure you want to continue?
```

The following example shows how to verify client access between mesh access points *SB_MAP1* and *SB_RAP2* at *36 Mbps*, *20 fps*, *100 frame size*, and *15-second* duration:

```
(Cisco Controller) >config mesh linktest SB_MAP1 SB_RAP1 36 20 100 15
LinkTest started on source AP, test ID: 0
[00:1D:71:0E:85:00]->[00:1D:71:0E:D0:0F]
Test config: 100 byte packets at 20 pps for 15 seconds, a-link rate 36 Mb/s
In progress: | || || || || || || |
LinkTest complete
Results
=====
txPkts:                290
txBuffAllocErr:        0
txQFullErrs:           0
Total rx pkts heard at destination:      290
rx pkts decoded correctly:
  err pkts: Total      0 (PHY 0 + CRC 0 + Unknown 0), TooBig 0, TooSmall 0
  rx lost packets:     0 (incr for each pkt seq missed or out of order)
  rx dup pkts:         0
  rx out of order:     0
avgSNR:   37, high: 40, low: 5
SNR profile [0dB...60dB]
   0          1          0          0          1
   3          0          1          0          2
   8          27         243         4          0
   0          0          0          0          0
(>60dB)      0
avgNf:   -89, high: -58, low: -90
Noise Floor profile [-100dB...-40dB]
   0          0          0          145         126
  11         2          0          1          0
   3          0          1          0          1
   0          0          0          0          0
(>-40dB)     0
avgRssi:  51, high: 53, low: 50
RSSI profile [-100dB...-40dB]
   0          0          0          0          0
   0          0          0          0          0
   0          0          0          0          0
   0          7         283         0          0
(>-40dB)     0
Summary PktFailedRate (Total pkts sent/recvd):      0.000%
Physical layer Error rate (Total pkts with errors/Total pkts heard): 0.000%
```

The following table lists the output flags displayed for the **config mesh linktest** command.

Table 1: Output Flags for the Config Mesh Linktest Command

Output Flag	Description
txPkts	Number of packets sent by the source.
txBuffAllocErr	Number of linktest buffer allocation errors at the source (expected to be zero).
txQFullErrs	Number of linktest queue full errors at the source (expected to be zero).
Total rx pkts heard at destination	Number of linktest packets received at the destination (expected to be same as or close to the txPkts).

Output Flag	Description
rx pkts decoded correctly	Number of linktest packets received and decoded correctly at the destination (expected to be same as close to txPkts).
err pkts: Total	Packet error statistics for linktest packets with errors.
rx lost packets	Total number of linktest packets not received at the destination.
rx dup pkts	Total number of duplicate linktest packets received at the destination.
rx out of order	Total number of linktest packets received out of order at the destination.
avgNF	Average noise floor.
Noise Floor profile	Noise floor profile in dB and are negative numbers.
avgSNR	Average SNR values.
SNR profile [odb...60dB]	Histogram samples received between 0 to 60 dB. The different colums in the SNR profile is the number of packets falling under the bucket 0-3, 3-6, 6-9, up to 57-60.
avgRSSI	Average RSSI values. The average high and low RSSI values are positive numbers.
RSSI profile [-100dB...-40dB]	The RSSI profile in dB and are negative numbers.

config mesh lsc

To configure a locally significant certificate (LSC) on mesh access points, use the **config mesh lsc** command.

```
config mesh lsc {enable | disable}
```

Syntax Description	enable	Enables an LSC on mesh access points.
	disable	Disables an LSC on mesh access points.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable LSC on mesh access points:

```
(Cisco Controller) >config mesh lsc enable
```

config mesh lsc advanced

To configure an advanced locally significant certificate (LSC) when a wildcard is used in an external authentication, authorization, and accounting (AAA) server for a mesh Access Point (AP), use the **config mesh lsc advanced** command.

```
config mesh lsc advanced {enable | disable}
```

Syntax Description	
enable	Enables advanced LSC for a mesh AP.
disable	Disables advanced LSC for a mesh AP.

Command Default	
	None

Command History	Release	Modification
	8.0	This command was introduced.

The following example shows how to enable advanced LSC for a mesh AP:

```
(Cisco Controller) >config mesh lsc advanced enable
```

config mesh lsc advanced ap-provision

To configure advanced mesh locally significant certificate (LSC) Access Point (AP) provision if a wildcard is used in an external authentication, authorization, and accounting (AAA) server for a mesh AP, use the **config mesh lsc advanced ap-provision** command.

```
config mesh lsc advanced ap-provision {enable | disable | open-window {enable | disable} | provision-controller {enable | disable}}
```

Syntax Description	enable	disable	open-window	enable	disable	provision-controller	enable	disable
	Enables advanced mesh LSC AP provision if a wildcard is used in an external AAA server for a mesh AP.	Disables advanced mesh LSC AP provision if a wildcard is used in an external AAA server for a mesh AP .	Configures mesh LSC provision for all mesh APs without MAC validation.	Enables AP provision for all mesh APs without MAC validation.	Disables AP provision for all mesh APs without MAC validation.	Configures the provision controller details for mesh APs to get an LSC.	Enables the provision controller option to get an LSC.	Disables the provision controller option to get an LSC.

Command Default None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to enable the advanced AP provision method:

```
(Cisco Controller) >config mesh lsc advanced ap-provision enable
```

config mesh multicast

To configure multicast mode settings to manage multicast transmissions within the mesh network, use the **config mesh multicast** command.

config mesh multicast { **regular** | **in** | **in-out** }

Syntax Description	regular	
		Multicasts the video across the entire mesh network and all its segments by bridging-enabled root access points (RAPs) and mesh access points (MAPs).
	in	Forwards the multicast video received from the Ethernet by a MAP to the RAP's Ethernet network. No additional forwarding occurs, which ensures that non-LWAPP 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 they are filtered out
	in-out	Configures the RAP and MAP to multicast, but each 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 Ethernets, 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. See the Usage Guidelines section for more information.
Command Default	In-out mode	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Multicast for mesh networks cannot be enabled using the controller GUI.

Mesh multicast modes determine how bridging-enabled access points mesh access points (MAPs) and root access points (RAPs) send multicasts among Ethernet LANs within a mesh network. Mesh multicast modes manage non-LWAPP multicast traffic only. LWAPP multicast traffic is governed by a different mechanism.

You can use the controller CLI to configure three mesh multicast modes to manage video camera broadcasts on all mesh access points. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

When using in-out mode, 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.



Note If 802.11b clients need to receive CAPWAP multicasts, then multicast must be enabled globally on the controller as well as on the mesh network (by using the **config network multicast global** command). If multicast does not need to extend to 802.11b clients beyond the mesh network, you should disable the global multicast parameter.

The following example shows how to multicast video across the entire mesh network and all its segments by bridging-enabled RAPs and MAPs:

```
(Cisco Controller) >config mesh multicast regular
```

config mesh parent preferred

To configure a preferred parent for a mesh access point, use the **config mesh parent preferred** command.

```
config mesh parent preferred cisco_ap {mac_address | none}
```

Syntax Description		
<i>cisco_ap</i>	Name of the child access point.	
<i>mac_address</i>	MAC address of the preferred parent.	
none	Clears the configured parent.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

A child AP selects the preferred parent based on the following conditions:

- The preferred parent is the best parent.
- The preferred parent has a link SNR of at least 20 dB (other parents, however good, are ignored).
- The preferred parent has a link SNR in the range of 12 dB and 20 dB, but no other parent is significantly better (that is, the SNR is more than 20 percent better). For an SNR lower than 12 dB, the configuration is ignored.
- The preferred parent is not in a blocked list.
- The preferred parent is not in silent mode because of dynamic frequency selection (DFS).
- The preferred parent is in the same bridge group name (BGN). If the configured preferred parent is not in the same BGN and no other parent is available, the child joins the parent AP using the default BGN.

The following example shows how to configure a preferred parent with the MAC address 00:21:1b:ea:36:60 for a mesh access point myap1:

```
(Cisco Controller) >config mesh parent preferred myap1 00:21:1b:ea:36:60
```

The following example shows how to clear a preferred parent with the MAC address 00:21:1b:ea:36:60 for a mesh access point myap1, by using the keyword none:

```
(Cisco Controller) >config mesh parent preferred myap1 00:21:1b:ea:36:60 none
```

config mesh public-safety

To enable or disable the 4.9-GHz public safety band for mesh access points, use the **config mesh public-safety** command.

```
config mesh public-safety {enable | disable} {all | cisco_ap}
```

Syntax Description		
enable		Enables the 4.9-GHz public safety band.
disable		Disables the 4.9-GHz public safety band.
all		Applies the command to all mesh access points.
<i>cisco_ap</i>		Specific mesh access point.

Command Default The 4.9-GHz public safety band is disabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines 4.9 GHz is a licensed frequency band restricted to public-safety personnel.

The following example shows how to enable the 4.9-GHz public safety band for all mesh access points:

```
(Cisco Controller) >config mesh public-safety enable all
4.9GHz is a licensed frequency band in -A domain for public-safety usage
Are you sure you want to continue? (y/N) y
```

config mesh radius-server

To enable or disable external authentication for mesh access points, use the **config mesh radius-server** command.

config mesh radius-server *index* { **enable** | **disable** }

Syntax Description	<i>index</i>	RADIUS authentication method. Options are as follows: <ul style="list-style-type: none"> • Enter eap to designate Extensible Authentication Protocol (EAP) for the mesh RADIUS server setting. • Enter psk to designate Preshared Keys (PSKs) for the mesh RADIUS server setting.
	enable	Enables the external authentication for mesh access points.
	disable	Disables the external authentication for mesh access points.
Command Default	EAP is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable external authentication for mesh access points:

```
(Cisco Controller) >config mesh radius-server eap enable
```


config mesh range

To globally set the maximum range between outdoor root access points (RAPs) and mesh access points (MAPs), use the **config mesh range** command.

config mesh range [*distance*]

Syntax Description	<i>distance</i>	(Optional) Maximum operating range (150 to 132000 ft) of the mesh access point.
Command Default	12,000 feet.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	After this command is enabled, all outdoor mesh access points reboot. This command does not affect indoor access points.	

The following example shows how to set the range between an outdoor mesh RAP and a MAP:

```
(Cisco Controller) >config mesh range 300
Command not applicable for indoor mesh. All outdoor Mesh APs will be rebooted
Are you sure you want to start? (y/N) y
```

config mesh secondary-backhaul

To configure a secondary backhaul on the mesh network, use the **config mesh secondary-backhaul** command.

```
config mesh secondary-backhaul { enable [force-same-secondary-channel] | disable [rll-retransmit | rll-transmit] }
```

Syntax Description

enable	Enables the secondary backhaul configuration.
force-same-secondary- channel	(Optional) Enables secondary-backhaul mesh capability. Forces all access points rooted at the first hop node to have the same secondary channel and ignores the automatic or manual channel assignments for the mesh access points (MAPs) at the second hop and beyond.
disable	Specifies the secondary backhaul configuration is disabled.
rll-transmit	(Optional) Uses reliable link layer (RLL) at the second hop and beyond.
rll-retransmit	(Optional) Extends the number of RLL retry attempts in an effort to improve reliability.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command uses a secondary backhaul radio as a temporary path for traffic that cannot be sent on the primary backhaul due to intermittent interference.

The following example shows ho to enable a secondary backhaul radio and force all access points rooted at the first hop node to have the same secondary channel:

```
(Cisco Controller) >config mesh secondary-backhaul enable force-same-secondary-channel
```

config mesh security

To configure the security settings for mesh networks, use the **config mesh security** command.

```
config mesh security {{rad-mac-filter | force-ext-auth } {enable | disable}} | {{eap | psk provisioning | provisioning window} | {enable | disable}} | {delete_psk | key}
```

Syntax Description		
rad-mac-filter		Enables a Remote Authentication Dial-In User Service (RADIUS) MAC address filter for the mesh security setting.
force-ext-auth		Disables forced external authentication for the mesh security setting.
lsc-only-auth		Enables Locally Significant Certificate only authentication for the mesh security setting.
enable		Enables the mesh security setting.
disable		Disables the mesh security setting.
eap		Designates the Extensible Authentication Protocol (EAP) for the mesh security setting by default.
psk		Designates a preshared key(PSK) for the mesh security setting.
provisioning		Encrypts provisioning for the PSK in Cisco Wireless Controller (WLC).
provisioning window		Encrypts provisioning window for the PSK in Cisco WLC.
enable		Enables provisioning of the PSK.
disable		Disables provisioning of the PSK.
key		Specifies the key for the PSK.

Command Default The EAP is designated as default for the mesh security.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.2	This command was modified, the psk provisioning and psk provisioning keywords are added.

The following example shows how to configure EAP as the security option for all mesh access points:

```
(Cisco Controller) config mesh security eap
```

The following example shows how to configure PSK as the security option for all mesh access points:

```
(Cisco Controller) config mesh security psk
```

The following example shows how to enable PSK provisioning as the security option for all mesh access points:

```
(Cisco Controller) > config mesh security psk provisioning enable
```

The following example shows how to configure a PSK provisioning key as the security option for all mesh access points:

```
(Cisco Controller) > config mesh security psk provisioning key 5
```

The following example shows how to enable a PSK provisioning window as the security option for all mesh access points:

```
(Cisco Controller) > config mesh security psk provisioning window enable
```

The following example shows how to delete the PSK provisioning for Cisco WLC :

```
(Cisco Controller) > config mesh security psk provisioning delete_psk wlc
```

The following example shows how to delete the PSK provisioning for all mesh access points:

```
(Cisco Controller) > config mesh security psk provisioning delete_psk ap
```

The following example shows how to delete PSK provisioning for all configurations in Cisco WLC :

```
(Cisco Controller) > config mesh security psk provisioning delete_psk wlc all
```

config mesh slot-bias

To enable or disable slot bias for serial backhaul mesh access points, use the **config mesh slot-bias** command.

config mesh slot-bias {enable | disable}

Syntax Description	enable	Enables slot bias for serial backhaul mesh APs.
	disable	Disables slot bias for serial backhaul mesh APs.
Command Default	By default, slot bias is in enabled state.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Follow these guidelines when using this command:

- The **config mesh slot-bias** command is a global command and therefore applicable to all 1524SB APs associated with the same controller.
- Slot bias is applicable only when both slot 1 and slot 2 are available. If a slot radio does not have a channel that is available because of dynamic frequency selection (DFS), the other slot takes up both the uplink and downlink roles.
- If slot 2 is not available because of hardware issues, slot bias functions normally. Corrective action should be taken by disabling the slot bias or fixing the antenna.

The following example shows how to disable slot bias for serial backhaul mesh APs:

```
(Cisco Controller) >config mesh slot-bias disable
```

debug mesh security

To configure the debugging of mesh security issues, use the **debug mesh security** command.

debug mesh security {all | events | errors} {enable | disable}

Syntax Description

all	Configures the debugging of all mesh security messages.
events	Configures the debugging of mesh security event messages.
errors	Configures the debugging of mesh security error messages.
enable	Enables the debugging of mesh security error messages.
disable	Disables the debugging of mesh security error messages.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of mesh security error messages:

```
(Cisco Controller) >debug mesh security errors enable
```

show mesh ap

To display settings for mesh access points, use the **show mesh ap** command.

show mesh ap {**summary** | **tree**}

Syntax Description	summary	tree
	Displays a summary of mesh access point information including the name, model, bridge virtual interface (BVI) MAC address, United States Computer Emergency Response Team (US-CERT) MAC address, hop, and bridge group name.	Displays a summary of mesh access point information in a tree configuration, including the name, hop counter, link signal-to-noise ratio (SNR), and bridge group name.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary format:

```
(Cisco Controller) >show mesh ap summary
AP Name AP Model BVI MAC CERT MAC Hop Bridge Group Name
-----
SB_RAP1 AIR-LAP1522AG-A-K9 00:1d:71:0e:d0:00 00:1d:71:0e:d0:00 0 sbox
SB_MAP1 AIR-LAP1522AG-A-K9 00:1d:71:0e:85:00 00:1d:71:0e:85:00 1 sbox
SB_MAP2 AIR-LAP1522AG-A-K9 00:1b:d4:a7:8b:00 00:1b:d4:a7:8b:00 2 sbox
SB_MAP3 AIR-LAP1522AG-A-K9 00:1d:71:0d:ee:00 00:1d:71:0d:ee:00 3 sbox
Number of Mesh APs..... 4
Number of RAPs..... 1
Number of MAPs..... 3
```

The following example shows how to display settings in a hierarchical (tree) format:

```
(Cisco Controller) >show mesh ap tree
=====
|| AP Name [Hop Counter, Link SNR, Bridge Group Name] ||
=====
[Sector 1]
-----
SB_RAP1[0,0,sbox]
|-SB_MAP1[1,32,sbox]
| |-SB_MAP2[2,27,sbox]
| |-SB_MAP3[3,30,sbox]
-----
Number of Mesh APs..... 4
Number of RAPs..... 1
Number of MAPs..... 3
-----
```

Related Topics

[config mesh alarm](#), on page 3

[config mesh astools](#), on page 4

[config mesh battery-state](#), on page 7

show mesh astools stats

To display antistranding statistics for outdoor mesh access points, use the **show mesh astools stats** command.

```
show mesh astools stats [cisco_ap]
```

Syntax Description	<i>cisco_ap</i>	(Optional) Antistranding feature statistics for a designated mesh access point.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display anti-stranding statistics on all outdoor mesh access points:

```
(Cisco Controller) >show mesh astools stats
Total No of Aps stranded : 0
```

The following example shows how to display anti-stranding statistics for access point *sb_map1*:

```
(Cisco Controller) >show mesh astools stats sb_map1
Total No of Aps stranded : 0
```

Related Topics

- [show mesh config](#), on page 38
- [show mesh stats](#), on page 49
- [config mesh astools](#), on page 4

show mesh backhaul

To check the current backhaul information, use the **show mesh backhaul** command.

show mesh backhaul *cisco_ap*

Syntax Description	<i>cisco_ap</i>	Name of the access point.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the current backhaul:

```
(Cisco Controller) >show mesh backhaul
```

If the current backhaul is 5 GHz, the output is as follows:

```
Basic Basic Attributes for Slot 0
  Radio Type..... RADIO_TYPE_80211g
  Radio Role..... DOWNLINK_ACCESS
  Administrative State ..... ADMIN_ENABLED
  Operation State ..... UP
  Current Tx Power Level ..... 1
If the current backhaul is 2.4 GHz, the output is as follows:
Basic Attributes for Slot 1
  Radio Type..... RADIO_TYPE_80211a
  Radio Subband..... RADIO_SUBBAND_ALL
  Radio Role..... DOWNLINK_ACCESS
  Administrative State ..... ADMIN_ENABLED
  Operation State ..... UP
  Current Tx Power Level ..... 1
  Current Channel ..... 165
  Antenna Type..... EXTERNAL_ANTENNA
  External Antenna Gain (in .5 dBm units).... 0
Current Channel.....6
Antenna Type.....External_ANTENNA
External Antenna Gain (in .5 dBm units).....0
```

Related Topics

[show mesh config](#), on page 38

[show mesh stats](#), on page 49

[config mesh astools](#), on page 4

show mesh cac

To display call admission control (CAC) topology and the bandwidth used or available in a mesh network, use the **show mesh cac** command.

```
show mesh cac {summary | {bwused {voice | video} | access | callpath | rejected}
cisco_ap}
```

Syntax Description	summary	Displays the total number of voice calls and voice bandwidth used for each mesh access point.
	bwused	Displays the bandwidth for a selected access point in a tree topology.
	voice	Displays the mesh topology and the voice bandwidth used or available.
	video	Displays the mesh topology and the video bandwidth used or available.
	access	Displays access voice calls in progress in a tree topology.
	callpath	Displays the call bandwidth distributed across the mesh tree.
	rejected	Displays voice calls rejected for insufficient bandwidth in a tree topology.
	<i>cisco_ap</i>	Mesh access point name.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of the call admission control settings:

```
(Cisco Controller) >show mesh cac summary
AP Name          Slot#   Radio  BW Used/Max  Calls
-----
SB_RAP1          0       11b/g  0/23437      0
                  1       11a    0/23437      0
SB_MAP1          0       11b/g  0/23437      0
                  1       11a    0/23437      0
SB_MAP2          0       11b/g  0/23437      0
                  1       11a    0/23437      0
SB_MAP3          0       11b/g  0/23437      0
                  1       11a    0/23437      0
```

The following example shows how to display the mesh topology and the voice bandwidth used or available:

```
(Cisco Controller) >show mesh cac bwused voice SB_MAP1
AP Name           Slot#   Radio   BW Used/Max
-----
  SB_RAP1         0      11b/g   0/23437
                  1      11a     0/23437
|  SB_MAP1        0      11b/g   0/23437
                  1      11a     0/23437
|| SB_MAP2        0      11b/g   0/23437
                  1      11a     0/23437
||| SB_MAP3       0      11b/g   0/23437
                   1      11a     0/23437
```

The following example shows how to display the access voice calls in progress in a tree topology:

```
(Cisco Controller) >show mesh cac access 1524_Map1
AP Name           Slot#   Radio   Calls
-----
  1524_Rap        0      11b/g   0
                  1      11a     0
                  2      11a     0
|  1524_Map1      0      11b/g   0
                  1      11a     0
                  2      11a     0
|| 1524_Map2     0      11b/g   0
                  1      11a     0
                  2      11a     0
```

show mesh client-access

To display the backhaul client access configuration setting, use the **show mesh client-access** command.

show mesh client-access

Syntax Description This command has no arguments or keywords.

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display backhaul client access configuration settings for a mesh access point:

```
(Cisco Controller) >show mesh client-access
Backhaul with client access status: enabled
Backhaul with client access extended status(3 radio AP): disabled
```

Related Topics

[config mesh client-access](#), on page 8

show mesh config

To display mesh configuration settings, use the **show mesh config** command.

show mesh config

Syntax Description This command has no arguments or keywords.

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display global mesh configuration settings:

```
(Cisco Controller) >show mesh config
Mesh Range..... 12000
Mesh Statistics update period..... 3 minutes
Backhaul with client access status..... disabled
Backhaul with extended client access status..... disabled
Background Scanning State..... enabled
Backhaul Amsdu State..... disabled
Mesh Security
  Security Mode..... EAP
  External-Auth..... disabled
  Use MAC Filter in External AAA server..... disabled
  Force External Authentication..... disabled
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
  Association Interval..... 60 minutes
  Parent Change Numbers..... 3
Parent Change Interval..... 60 minutes
Mesh Multicast Mode..... In-Out
Mesh Full Sector DFS..... enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... disabled
Mesh DCA channels for serial backhaul APs..... enabled
Mesh Slot Bias..... enabled
```

Related Topics

[show mesh astools stats](#), on page 33

[show mesh stats](#), on page 49

[config mesh astools](#)

show mesh env

To display global or specific environment summary information for mesh networks, use the **show mesh env** command.

```
show mesh env {summary | cisco_ap}
```

Syntax Description	summary	Displays global environment summary information.
	<i>cisco_ap</i>	Name of access point for which environment summary information is requested.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display global environment summary information:

```
(Cisco Controller) >show mesh env summary
AP Name           Temperature(C)  Heater  Ethernet  Battery
-----
ap1130:5f:be:90   N/A            N/A     DOWN      N/A
AP1242:b2.31.ea   N/A            N/A     DOWN      N/A
AP1131:f2.8d.92   N/A            N/A     DOWN      N/A
AP1131:46f2.98ac  N/A            N/A     DOWN      N/A
ap1500:62:39:70   -36            OFF     UP        N/A
```

The following example shows how to display an environment summary for an access point:

```
(Cisco Controller) >show mesh env SB_RAP1
AP Name..... SB_RAP1
AP Model..... AIR-LAP1522AG-A-K9
AP Role..... RootAP
Temperature..... 21 C, 69 F
Heater..... OFF
Backhaul..... GigabitEthernet0
GigabitEthernet0 Status..... UP
    Duplex..... FULL
    Speed..... 100
    Rx Unicast Packets..... 114754
    Rx Non-Unicast Packets..... 1464
    Tx Unicast Packets..... 9630
    Tx Non-Unicast Packets..... 3331
GigabitEthernet1 Status..... DOWN
    POE Out..... OFF
Battery..... N/A
```

show mesh neigh

To display summary or detailed information about the mesh neighbors of a mesh access point, use the **show mesh neigh** command.

```
show mesh neigh {detail | summary} {cisco_ap | all}
```

Syntax Description	detail	Description
	detail	Displays the channel and signal-to-noise ratio (SNR) details between the designated mesh access point and its neighbor.
	summary	Displays the mesh neighbors for a designated mesh access point.
	<i>cisco_ap</i>	Cisco lightweight access point name.
	all	Displays all access points.



Note

If an AP itself is configured with the **all** keyword, the **all** keyword access points take precedence over the AP that is named **all**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a neighbor summary of an access point:

```
(Cisco Controller) >show mesh neigh summary RAP1
AP Name/Radio Mac Channel Rate Link-Snr Flags State
-----
00:1D:71:0F:CA:00 157 54 6 0x0 BEACON
00:1E:14:48:25:00 157 24 1 0x0 BEACON
MAP1-BB00 157 54 41 0x11 CHILD BEACON
```

The following example shows how to display the detailed neighbor statistics of an access point:

```
(Cisco Controller) >show mesh neigh detail RAP1
AP MAC : 00:1E:BD:1A:1A:00 AP Name: HOR1522_MINE06_MAP_S_Dyke
backhaul rate 54
FLAGS : 860 BEACON
worstDv 255, Ant 0, channel 153, biters 0, ppiters 0
Numroutes 0, snr 0, snrUp 8, snrDown 8, linkSnr 8
adjustedEase 0, unadjustedEase 0
txParent 0, rxParent 0
poorSnr 0
lastUpdate 2483353214 (Sun Aug 4 23:51:58 1912)
parentChange 0
Per antenna smoothed snr values: 0 0 0 0
Vector through 00:1E:BD:1A:1A:00
```

The following table lists the output flags displayed for the **show mesh neigh detail** command.

Table 2: Output Flags for the show mesh neigh detail command

Output Flag	Description
AP MAC	MAC address of a mesh neighbor for a designated mesh access point.
AP Name	Name of the mesh access point.
FLAGS	Describes adjacency. The possible values are as follows: <ul style="list-style-type: none"> • UPDATED—Recently updated neighbor. • NEIGH—One of the top neighbors. • EXCLUDED—Neighbor is currently excluded. • WASEXCLUDED—Neighbor was recently removed from the exclusion list. • PERMSNR—Permanent SNR neighbor. • CHILD—A child neighbor. • PARENT—A parent neighbor. • NEEDUPDATE—Not a current neighbor and needs an update. • BEACON—Heard a beacon from this neighbor. • ETHER—Ethernet neighbor.
worstDv	Worst distance vector through the neighbor.
Ant	Antenna on which the route was received.
channel	Channel of the neighbor.
biters	Number of black list timeouts left.
ppiters	Number of potential parent timeouts left.
Numroutes	Number of distance routes.
snr	Signal to Noise Ratio.
snrUp	SNR of the link to the AP.
snrDown	SNR of the link from the AP.
linkSnr	Calculated SNR of the link.
adjustedEase	Ease to the root AP through this AP. It is based on the current SNR and threshold SNR values.

Output Flag	Description
unadjustedEase	Ease to the root AP through this AP after applying correct for number of hops.
txParent	Packets sent to this node while it was a parent.
rxparent	Packets received from this node while it was a parent.
poorSnr	Packets with poor SNR received from a node.
lastUpdate	Timestamp of the last received message for this neighbor
parentChange	When this node last became parent.
per antenna smoother SNR values	SNR value is populated only for antenna 0.

show mesh path

To display the channel and signal-to-noise ratio (SNR) details for a link between a mesh access point and its neighbor, use the **show mesh path** command.

show mesh path *cisco_ap*

Syntax Description	<i>cisco_ap</i>	Mesh access point name.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display channel and SNR details for a designated link path:

```
(Cisco Controller) >show mesh path mesh-45-rap1
AP Name/Radio Mac Channel Rate Link-Snr Flags State
-----
MAP1-BB00          157    54    32    0x0    UPDATED NEIGH PARENT BEACON
RAP1                157    54    37    0x0    BEACON
```

show mesh per-stats

To display the percentage of packet errors for packets transmitted by the neighbors of a specified mesh access point, use the **show mesh per-stats** command.

show mesh per-stats summary {*cisco_ap* | **all**}

Syntax Description		
	summary	Displays the packet error rate stats summary.
	<i>cisco_ap</i>	Name of mesh access point.
	all	Displays all mesh access points.



Note If an AP itself is configured with the **all** keyword, the **all** keyword access points take precedence over the AP that is named **all**.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines The packet error rate percentage equals 1, which is the number of successfully transmitted packets divided by the number of total packets transmitted.

The following example shows how to display the percentage of packet errors for packets transmitted by the neighbors to a mesh access point:

```
(Cisco Controller) >show mesh per-stats summary ap_12
Neighbor MAC Address 00:0B:85:5F:FA:F0
Total Packets transmitted: 104833
Total Packets transmitted successfully: 104833
Total Packets retried for transmission: 33028
RTS Attempts: 0
RTS Success: 0
Neighbor MAC Address: 00:0B:85:80:ED:D0
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
Neighbor MAC Address: 00:17:94:FE:C3:5F
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
RTS Attempts: 0
RTS Success: 0
```

show mesh public-safety

To display 4.8-GHz public safety settings, use the **show mesh public-safety** command.

show mesh public-safety

Syntax Description This command has no arguments or keywords.

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to view 4.8-GHz public safety settings:

```
(Cisco Controller) >(Cisco Controller) >show mesh public-safety  
Global Public Safety status: disabled
```

Related Topics

[config mesh public-safety](#), on page 23

show mesh queue-stats

To display the number of packets in a client access queue by type for a mesh access point, use the **show mesh queue-stats** command.

show mesh queue-stats { *cisco_ap* | **all** }



Note If an AP itself is configured with the **all** keyword, the **all** keyword access points take precedence over the AP that is named **all**.

Syntax Description		
<i>cisco_ap</i>	Name of access point for which you want packet queue statistics.	
all	Displays all access points.	

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.


The following example shows how to display packet queue statistics for access point ap417:

```
(Cisco Controller) >show mesh queue-stats ap417
Queue Type Overflows Peak length Average length
-----
Silver      0           1           0.000
Gold        0           4           0.004
Platinum    0           4           0.001
Bronze      0           0           0.000
Management 0           0           0.000
```

show mesh security-stats

To display packet error statistics for a specific access point, use the **show mesh security-stats** command.

```
show mesh security-stats { cisco_ap | all }
```

Syntax Description	<i>cisco_ap</i>	Name of access point for which you want packet error statistics.
	all	Displays all access points.
		
Note	If an AP itself is configured with the all keyword, the all keyword access points take precedence over the AP that is named all .	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	This command shows packet error statistics and a count of failures, timeouts, and successes with respect to associations and authentications as well as reassociations and reauthentications for the specified access point and its child.	

The following example shows how to view packet error statistics for access point ap417:

```
(Cisco Controller) >show mesh security-stats ap417
AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
-----
x Packets 14, Rx Packets 19, Rx Error Packets 0
Parent-Side Statistics:
-----
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Child-Side Statistics:
-----
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
Re-Association Timeouts 0
Re-Association Successes 0
Re-Authentication Failures 0
```

```
Re-Authentication Timeouts 0  
Re-Authentication Successes 0
```

Related Topics

[config mesh security](#), on page 27

show mesh stats

To display the mesh statistics for an access point, use the **show mesh stats** command.

```
show mesh stats cisco_ap
```

Syntax Description	<i>cisco_ap</i>	Access point name.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display statistics of an access point:

```
(Cisco Controller) >show mesh stats RAP_AP1
RAP in state Maint
rxNeighReq 759978, rxNeighRsp 568673
txNeighReq 115433, txNeighRsp 759978
rxNeighUpd 8266447 txNeighUpd 693062
tnextchan 0, nextant 0, downAnt 0, downChan 0, curAnts 0
tnextNeigh 0, malformedNeighPackets 244, poorNeighSnr 27901
blacklistPackets 0, insufficientMemory 0
authenticationFailures 0
Parent Changes 1, Neighbor Timeouts 16625
```

show mesh stats