



LWAP Commands

- [capwap ap controller ip address, on page 5](#)
- [capwap ap dot1x, on page 6](#)
- [capwap ap hostname, on page 7](#)
- [capwap ap ip address, on page 8](#)
- [capwap ap ip default-gateway, on page 9](#)
- [capwap ap log-server, on page 10](#)
- [capwap ap primary-base, on page 11](#)
- [capwap ap primed-timer, on page 12](#)
- [lwapp ap controller ip address, on page 13](#)
- [config 802.11-a antenna extAntGain, on page 14](#)
- [config 802.11-a channel ap, on page 15](#)
- [config 802.11-a txpower ap, on page 16](#)
- [config 802.11 antenna diversity, on page 17](#)
- [config 802.11 antenna extAntGain, on page 18](#)
- [config 802.11 antenna mode, on page 19](#)
- [config 802.11 antenna selection, on page 20](#)
- [config 802.11 beamforming, on page 21](#)
- [config 802.11 disable, on page 22](#)
- [config advanced 802.11 profile clients, on page 23](#)
- [config advanced 802.11 profile customize, on page 24](#)
- [config advanced 802.11 profile foreign, on page 25](#)
- [config advanced 802.11 profile noise, on page 26](#)
- [config advanced 802.11 profile throughput, on page 27](#)
- [config advanced 802.11 profile utilization, on page 28](#)
- [config advanced backup-controller secondary, on page 29](#)
- [config advanced client-handoff, on page 30](#)
- [config advanced dot11-padding, on page 31](#)
- [config advanced assoc-limit, on page 32](#)
- [config advanced max-1x-sessions, on page 33](#)
- [config advanced probe backoff, on page 34](#)
- [config advanced probe filter, on page 35](#)
- [config advanced probe limit, on page 36](#)
- [config advanced timers, on page 37](#)

- [config ap](#), on page 40
- [config ap cdp](#), on page 41
- [config ap core-dump](#), on page 43
- [config ap crash-file clear-all](#), on page 44
- [config ap crash-file delete](#), on page 45
- [config ap crash-file get-crash-file](#), on page 46
- [config ap crash-file get-radio-core-dump](#), on page 47
- [config ap ethernet tag](#), on page 48
- [config ap image swap](#), on page 49
- [config ap led-state](#), on page 50
- [config ap location](#), on page 51
- [config ap logging syslog level](#), on page 52
- [config ap mgmtuser add](#), on page 53
- [config ap mgmtuser delete](#), on page 55
- [config ap monitor-mode](#), on page 56
- [config ap name](#), on page 57
- [config ap packet-dump](#), on page 58
- [config ap port](#), on page 61
- [config ap power injector](#), on page 62
- [config ap power pre-standard](#), on page 63
- [config ap preferred-mode](#), on page 64
- [config ap primary-base](#), on page 65
- [config ap reporting-period](#), on page 66
- [config ap reset](#), on page 67
- [config ap retransmit interval](#), on page 68
- [config ap retransmit count](#), on page 69
- [config ap sniff](#), on page 70
- [config ap ssh](#), on page 71
- [config ap static-ip](#), on page 72
- [config ap stats-timer](#), on page 74
- [config ap syslog host global](#), on page 75
- [config ap syslog host specific](#), on page 76
- [config ap tcp-mss-adjust](#), on page 77
- [config ap telnet](#), on page 78
- [config ap timezone](#), on page 79
- [config ap username](#), on page 80
- [config ap venue](#), on page 81
- [config ap wlan](#), on page 86
- [config country](#), on page 87
- [config known ap](#), on page 88
- [clear ap config](#), on page 89
- [clear ap eventlog](#), on page 90
- [clear ap join stats](#), on page 91
- [clear ap tsm](#), on page 92
- [debug ap](#), on page 93
- [debug ap enable](#), on page 95


- [debug ap packet-dump](#), on page 96
- [debug ap show stats](#), on page 97
- [debug ap show stats video](#), on page 99
- [debug capwap](#), on page 100
- [debug lwapp console cli](#), on page 101
- [debug service ap-monitor](#), on page 102
- [reset system at](#), on page 103
- [reset system in](#), on page 104
- [reset system cancel](#), on page 105
- [reset system notify-time](#), on page 106
- [show advanced max-1x-sessions](#), on page 107
- [show advanced probe](#), on page 108
- [show advanced timers](#), on page 109
- [show ap auto-rf](#), on page 110
- [show ap cdp](#), on page 112
- [show ap channel](#), on page 114
- [show ap config](#), on page 115
- [show ap config general](#) , on page 121
- [show ap config global](#), on page 122
- [show ap core-dump](#), on page 123
- [show ap crash-file](#), on page 124
- [show ap data-plane](#), on page 125
- [show ap dtls-cipher-suite](#), on page 126
- [show ap ethernet tag](#), on page 127
- [show ap eventlog](#), on page 128
- [show ap image](#), on page 129
- [show ap inventory](#), on page 130
- [show ap join stats detailed](#), on page 131
- [show ap join stats summary](#), on page 132
- [show ap join stats summary all](#), on page 133
- [show ap led-state](#), on page 134
- [show ap led-flash](#), on page 135
- [show ap max-count summary](#), on page 136
- [show ap monitor-mode summary](#), on page 137
- [show ap module summary](#), on page 138
- [show ap packet-dump status](#), on page 139
- [show ap prefer-mode stats](#), on page 140
- [show ap retransmit](#), on page 141
- [show ap stats](#), on page 142
- [show ap summary](#), on page 145
- [show ap tcp-mss-adjust](#), on page 146
- [show ap wlan](#), on page 147
- [show auth-list](#), on page 148
- [show client ap](#), on page 149
- [show boot](#), on page 150
- [show country](#), on page 151

- [show country channels, on page 152](#)
- [show country supported, on page 153](#)
- [show dtls connections, on page 155](#)
- [show known ap, on page 156](#)
- [show msglog, on page 157](#)
- [show network summary, on page 158](#)
- [show watchlist, on page 160](#)

capwap ap controller ip address

To configure the controller IP address into the CAPWAP access point from the access point's console port, use the **capwap ap controller ip address** command.

capwap ap controller ip address *A.B.C.D*

| | | |
|---|---|-------------------------------|
| Syntax Description | <i>A.B.C.D</i> | IP address of the controller. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |
| Usage Guidelines | This command must be entered from an access point's console port. This command is applicable for IPv4 addresses only. | |
|  | | |
| Note | The access point must be running Cisco IOS Release 12.3(11)JX1 or later releases. | |

The following example shows how to configure the controller IP address 10.23.90.81 into the CAPWAP access point:

```
ap_console >capwap ap controller ip address 10.23.90.81
```

capwap ap dot1x

To configure the dot1x username and password into the CAPWAP access point from the access point's console port, use the **capwap ap dot1x** command.

capwap ap dot1x username *user_name* **password** *password*

| Syntax Description | | |
|--------------------|------------------|-----------------|
| | <i>user_name</i> | Dot1x username. |
| | <i>password</i> | Dot1x password. |

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

| Usage Guidelines | This command must be entered from an access point's console port. |
|------------------|---|
|------------------|---|



| Note | The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases. |
|------|--|
|------|--|

This example shows how to configure the dot1x username ABC and password pass01:

```
ap_console >capwap ap dot1x username ABC password pass01
```

capwap ap hostname

To configure the access point host name from the access point's console port, use the **capwap ap hostname** command.

capwap ap hostname *host_name*

| | | |
|---------------------------|------------------|-------------------------------|
| Syntax Description | <i>host_name</i> | Hostname of the access point. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

Usage Guidelines This command must be entered from an access point's console port.



Note The access point must be running Cisco IOS Release 12.3(11)JX1 or later releases. This command is available only for the Cisco Lightweight AP IOS Software recovery image (rcvk9w8) without any private-config. You can remove the private-config by using the **clear capwap private-config** command.

This example shows how to configure the hostname WLC into the capwap access point:

```
ap_console >capwap ap hostname WLC
```

capwap ap ip address

To configure the IP address into the CAPWAP access point from the access point's console port, use the **capwap ap ip address** command.

capwap ap ip address *A.B.C.D*

| | | |
|---------------------------|---|------------------------------|
| Syntax Description | <i>A.B.C.D</i> | IP address. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |
| Usage Guidelines | This command must be entered from an access point's console port. This command supports only IPv4 address format. | |



Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the IP address 10.0.0.1 into CAPWAP access point:

```
ap_console >capwap ap ip address 10.0.0.1
```


capwap ap ip default-gateway

To configure the default gateway from the access point's console port, use the **capwap ap ip default-gateway** command.

capwap ap ip default-gateway *A.B.C.D*

| | | |
|---------------------------|----------------|---|
| Syntax Description | <i>A.B.C.D</i> | Default gateway address of the capwap access point. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

Usage Guidelines This command must be entered from an access point's console port. This command supports only IPv4 address format.



Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the CAPWAP access point with the default gateway address 10.0.0.1:

```
ap_console >capwap ap ip default-gateway 10.0.0.1
```

capwap ap log-server

To configure the system log server to log all the CAPWAP errors, use the **capwap ap log-server** command.

capwap ap log-server *A.B.C.D*

| | | |
|---------------------------|---|----------------------------------|
| Syntax Description | <i>A.B.C.D</i> | IP address of the syslog server. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |
| Usage Guidelines | This command must be entered from an access point's console port. This command supports only IPv4 address format. | |



Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the syslog server with the IP address 10.0.0.1:

```
ap_console >capwap ap log-server 10.0.0.1
```

capwap ap primary-base

To configure the primary controller name and IP address into the CAPWAP access point from the access point's console port, use the **capwap ap primary-base** command.



Note This command configures the IPv4 and IPv6 address for Cisco Wave 2 APs.

capwap ap primary-base *WORD A.B.C.D*

| Syntax Description | | |
|--------------------|----------------|---------------------------------------|
| | <i>WORD</i> | Name of the primary controller. |
| | <i>A.B.C.D</i> | IP address of the primary controller. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines This command must be entered from an access point's console port in enable mode (elevated access).

This example shows how to configure the primary controller name WLC1 and primary controller IP address 209.165.200.225 into the CAPWAP access point:

```
ap_console >capwap ap primary-base WLC1 209.165.200.225
```

capwap ap primed-timer

To configure the primed timer into the CAPWAP access point, use the **capwap ap primed-timer** command.

capwap ap primed-timer { **enable** | **disable** }

| Syntax Description | enable | enable |
|--------------------|----------------|-------------------------------------|
| | | Enables the primed timer settings |
| | disable | Disables the primed timer settings. |

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

| Usage Guidelines | This command must be entered from an access point's console port. |
|------------------|---|
|------------------|---|



| Note | The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases. |
|------|--|
|------|--|

This example shows how to enable the primed-timer settings:

```
ap_console >capwap ap primed-timer enable
```

lwapp ap controller ip address

To configure the Cisco WLC IP address into the FlexConnect access point from the access point's console port, use the **lwapp ap controller ip address** command.

lwapp ap controller ip address *A.B.C.D*

| | | |
|---------------------------|----------------|-------------------------------|
| Syntax Description | <i>A.B.C.D</i> | IP address of the controller. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

Usage Guidelines

This command must be entered from an access point's console port. This command is applicable for IPv4 addresses only.

Prior to changing the FlexConnect configuration on an access point using the access point's console port, the access point must be in standalone mode (not connected to a controller) and you must remove the current LWAPP private configuration by using the **clear lwapp private-config** command.



Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

The following example shows how to configure the controller IP address 10.92.109.1 into the FlexConnect access point:

```
ap_console > lwapp ap controller ip address 10.92.109.1
```

config 802.11-a antenna extAntGain

To configure the external antenna gain for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a antenna extAntGain** commands.

config { **802.11-a49** | **802.11-a58** } **antenna extAntGain** *ant_gain* *cisco_ap* { **global** | *channel_no* }

| Syntax Description | | |
|--------------------|--|--|
| 802.11-a49 | | Specifies the 4.9-GHz public safety channel. |
| 802.11-a58 | | Specifies the 5.8-GHz public safety channel. |
| <i>ant_gain</i> | | Value in .5-dBi units (for instance, 2.5 dBi = 5). |
| <i>cisco_ap</i> | | Name of the access point to which the command applies. |
| global | | Specifies the antenna gain value to all channels. |
| <i>channel_no</i> | | Antenna gain value for a specific channel. |

Command Default Channel properties are disabled.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines Before you enter the **config 802.11-a antenna extAntGain** command, disable the 802.11 Cisco radio with the **config 802.11-a disable** command.

After you configure the external antenna gain, use the **config 802.11-a enable** command to reenable the 802.11 Cisco radio.

The following example shows how to configure an 802.11-a49 external antenna gain of 10 dBi for AP1:

```
(Cisco Controller) >config 802.11-a antenna extAntGain 10 AP1
```

Related Topics

[config 802.11-a channel ap](#), on page 15

config 802.11-a channel ap

To configure the channel properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a channel ap** command.

```
config {802.11-a49 | 802.11-a58} channel ap cisco_ap {global | channel_no}
```

| Syntax Description | | |
|--------------------|--|---|
| 802.11-a49 | | Specifies the 4.9-GHz public safety channel. |
| 802.11-a58 | | Specifies the 5.8-GHz public safety channel. |
| <i>cisco_ap</i> | | Name of the access point to which the command applies. |
| global | | Enables the Dynamic Channel Assignment (DCA) on all 4.9-GHz and 5.8-GHz subband radios. |
| <i>channel_no</i> | | Custom channel for a specific mesh access point. The range is 1 through 26, inclusive, for a 4.9-GHz band and 149 through 165, inclusive, for a 5.8-GHz band. |

Command Default Channel properties are disabled.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to set the channel properties:

```
(Cisco Controller) >config 802.11-a channel ap
```

Related Topics

[config 802.11-a antenna extAntGain](#), on page 14

[config 802.11-a](#)

config 802.11-a txpower ap

To configure the transmission power properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a txpower ap** command.

```
config {802.11-a49 | 802.11-a58} txpower ap cisco_ap {global | power_level}
```

| Syntax Description | | |
|--------------------|--|---|
| 802.11-a49 | | Specifies the 4.9-GHz public safety channel. |
| 802.11-a58 | | Specifies the 5.8-GHz public safety channel. |
| txpower | | Configures transmission power properties. |
| ap | | Configures access point channel settings. |
| <i>cisco_ap</i> | | Name of the access point to which the command applies. |
| global | | Applies the transmission power value to all channels. |
| <i>power_level</i> | | Transmission power value to the designated mesh access point. The range is from 1 to 5. |

Command Default The default transmission power properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point is disabled.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to configure an 802.11-a49 transmission power level of 4 for AP1:

```
(Cisco Controller) >config 802.11-a txpower ap 4 AP1
```

Related Topics

[config 802.11-a antenna extAntGain](#), on page 14

[config 802.11-a](#)

[config 802.11-a channel ap](#), on page 15

config 802.11 antenna diversity

To configure the diversity option for 802.11 antennas, use the **config 802.11 antenna diversity** command.

config 802.11{ a | b} **antenna diversity** {enable | sideA | sideB} *cisco_ap*

| Syntax Description | | |
|--------------------|---|------------------------------|
| a | Specifies the 802.11a network. | |
| b | Specifies the 802.11b/g network. | |
| enable | Enables the diversity. | |
| sideA | Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point left port. | |
| sideB | Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point right port. | |
| <i>cisco_ap</i> | Cisco lightweight access point name. | |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to enable antenna diversity for AP01 on an 802.11b network:

```
(Cisco Controller) >config 802.11a antenna diversity enable AP01
```

The following example shows how to enable diversity for AP01 on an 802.11a network, using an external antenna connected to the Cisco lightweight access point left port (sideA):

```
(Cisco Controller) >config 802.11a antenna diversity sideA AP01
```

Related Topics

[config 802.11-a](#)

config 802.11 antenna extAntGain

To configure external antenna gain for an 802.11 network, use the **config 802.11 antenna extAntGain** command.

config 802.11 { **a** | **b** } **antenna extAntGain** *antenna_gain* *cisco_ap*

| Syntax Description | | |
|---------------------|--|---|
| a | | Specifies the 802.11a network. |
| b | | Specifies the 802.11b/g network. |
| <i>antenna_gain</i> | | Antenna gain in 0.5 dBm units (for example, 2.5 dBm = 5). |
| <i>cisco_ap</i> | | Cisco lightweight access point name. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines Before you enter the **config 802.11 antenna extAntGain** command, disable the 802.11 Cisco radio with the **config 802.11 disable** command.

After you configure the external antenna gain, use the **config 802.11 enable** command to enable the 802.11 Cisco radio.

The following example shows how to configure an *802.11a* external antenna gain of *0.5 dBm* for *AP1*:

```
(Cisco Controller) >config 802.11 antenna extAntGain 1 AP1
```

Related Topics

[config 802.11-a](#)

config 802.11 antenna mode

To configure the Cisco lightweight access point to use one internal antenna for an 802.11 sectorized 180-degree coverage pattern or both internal antennas for an 802.11 360-degree omnidirectional pattern, use the **config 802.11 antenna mode** command.

```
config 802.11 { a | b } antenna mode { omni | sectorA | sectorB } cisco_ap
```

| Syntax Description | | |
|--------------------|-----------------|--|
| | a | Specifies the 802.11a network. |
| | b | Specifies the 802.11b/g network. |
| | omni | Specifies to use both internal antennas. |
| | sectorA | Specifies to use only the side A internal antenna. |
| | sectorB | Specifies to use only the side B internal antenna. |
| | <i>cisco_ap</i> | Cisco lightweight access point name. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to configure access point AP01 antennas for a 360-degree omnidirectional pattern on an 802.11b network:

```
(Cisco Controller) >config 802.11 antenna mode omni AP01
```

Related Topics

[config 802.11-a](#)

config 802.11 antenna selection

To select the internal or external antenna selection for a Cisco lightweight access point on an 802.11 network, use the **config 802.11 antenna selection** command.

config 802.11 { a | b } **antenna selection** { internal | external } *cisco_ap*

| Syntax Description | | |
|--------------------|-----------------|--------------------------------------|
| | a | Specifies the 802.11a network. |
| | b | Specifies the 802.11b/g network. |
| | internal | Specifies the internal antenna. |
| | external | Specifies the external antenna. |
| | <i>cisco_ap</i> | Cisco lightweight access point name. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to configure access point AP02 on an 802.11b network to use the internal antenna:

```
(Cisco Controller) >config 802.11a antenna selection internal AP02
```

Related Topics

[config 802.11-a](#)

config 802.11 beamforming

To enable or disable Beamforming (ClientLink) on the network or on individual radios, enter the **config 802.11 beamforming** command.

```
config 802.11 {a | b} beamforming {global | ap ap_name} {enable | disable}
```

| Syntax Description | | |
|--------------------|--|--|
| a | | Specifies the 802.11a network. |
| b | | Specifies the 802.11b/g network. |
| global | | Specifies all lightweight access points. |
| ap ap_name | | Specifies the Cisco access point name. |
| enable | | Enables beamforming. |
| disable | | Disables beamforming. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines When you enable Beamforming on the network, it is automatically enabled for all the radios applicable to that network type.

Follow these guidelines for using Beamforming:

- Beamforming is supported only for legacy orthogonal frequency-division multiplexing (OFDM) data rates (6, 9, 12, 18, 24, 36, 48, and 54 mbps).



Note Beamforming is not supported for complementary-code keying (CCK) data rates (1, 2, 5.5, and 11 Mbps).

- Beamforming is supported only on access points that support 802.11n (AP1250 and AP1140).
- Two or more antennas must be enabled for transmission.
- All three antennas must be enabled for reception.
- OFDM rates must be enabled.

If the antenna configuration restricts operation to a single transmit antenna, or if OFDM rates are disabled, Beamforming is not used.

The following example shows how to enable Beamforming on the 802.11a network:

```
(Cisco Controller) >config 802.11 beamforming global enable
```

config 802.11 disable

To disable radio transmission for an entire 802.11 network or for an individual Cisco radio, use the **config 802.11 disable** command.

config 802.11{ a | b } **disable** { **network** | *cisco_ap* }

Syntax Description

| | |
|-----------------|---|
| a | Configures the 802.11a on slot 1 and 802.11ac radio on slot 2. radio. |
| b | Specifies the 802.11b/g network. |
| network | Disables transmission for the entire 802.11a network. |
| <i>cisco_ap</i> | Individual Cisco lightweight access point radio. |

Command Default

The transmission is enabled for the entire network by default.

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

Usage Guidelines

- You must use this command to disable the network before using many config 802.11 commands.
- This command can be used any time that the CLI interface is active.

The following example shows how to disable the entire 802.11a network:

```
(Cisco Controller) >config 802.11a disable network
```

The following example shows how to disable access point AP01 802.11b transmissions:

```
(Cisco Controller) >config 802.11b disable AP01
```

config advanced 802.11 profile clients

To set the Cisco lightweight access point clients threshold between 1 and 75 clients, use the **config advanced 802.11 profile clients** command.

```
config advanced 802.11 { a | b } profile clients { global | cisco_ap } clients
```

| Syntax Description | | |
|--------------------|--|---|
| a | | Specifies the 802.11a network. |
| b | | Specifies the 802.11b/g network. |
| global | | Configures all 802.11a Cisco lightweight access points. |
| <i>cisco_ap</i> | | Cisco lightweight access point name. |
| <i>clients</i> | | 802.11a Cisco lightweight access point client threshold between 1 and 75 clients. |

Command Default The default Cisco lightweight access point clients threshold is 12 clients.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to set all Cisco lightweight access point clients thresholds to 25 clients:

```
(Cisco Controller) >config advanced 802.11 profile clients global 25
Global client count profile set.
```

The following example shows how to set the AP1 clients threshold to 75 clients:

```
(Cisco Controller) >config advanced 802.11 profile clients AP1 75
Global client count profile set.
```

config advanced 802.11 profile customize

To turn customizing on or off for an 802.11a Cisco lightweight access point performance profile, use the **config advanced 802.11 profile customize** command.

```
config advanced 802.11{a | b} profile customize cisco_ap {on | off}
```

| Syntax Description | | |
|--------------------|--|---|
| a | | Specifies the 802.11a/n network. |
| b | | Specifies the 802.11b/g/n network. |
| <i>cisco_ap</i> | | Cisco lightweight access point. |
| on | | Customizes performance profiles for this Cisco lightweight access point. |
| off | | Uses global default performance profiles for this Cisco lightweight access point. |

Command Default The default state of performance profile customization is Off.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to turn performance profile customization on for 802.11a Cisco lightweight access point AP1:

```
(Cisco Controller) >config advanced 802.11 profile customize AP1 on
```


config advanced 802.11 profile foreign

To set the foreign 802.11a transmitter interference threshold between 0 and 100 percent, use the **config advanced 802.11 profile foreign** command.

```
config advanced 802.11 { a | b } profile foreign { global | cisco_ap } percent
```

| Syntax Description | | |
|--------------------|-----------------|---|
| | a | Specifies the 802.11a network. |
| | b | Specifies the 802.11b/g network. |
| | global | Configures all 802.11a Cisco lightweight access points. |
| | <i>cisco_ap</i> | Cisco lightweight access point name. |
| | <i>percent</i> | 802.11a foreign 802.11a interference threshold between 0 and 100 percent. |

Command Default The default foreign 802.11a transmitter interference threshold value is 10.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to set the foreign 802.11a transmitter interference threshold for all Cisco lightweight access points to 50 percent:

```
(Cisco Controller) >config advanced 802.11a profile foreign global 50
```

The following example shows how to set the foreign 802.11a transmitter interference threshold for AP1 to 0 percent:

```
(Cisco Controller) >config advanced 802.11 profile foreign AP1 0
```

Related Topics

[config advanced 802.11 profile throughput](#), on page 27

config advanced 802.11 profile noise

To set the 802.11a foreign noise threshold between -127 and 0 dBm, use the **config advanced 802.11 profile noise** command.

config advanced 802.11{a | b} **profile noise** {global | cisco_ap} dBm

| Syntax Description | | |
|--------------------|--|--|
| a | | Specifies the 802.11a/n network. |
| b | | Specifies the 802.11b/g/n network. |
| global | | Configures all 802.11a Cisco lightweight access point specific profiles. |
| <i>cisco_ap</i> | | Cisco lightweight access point name. |
| <i>dBm</i> | | 802.11a foreign noise threshold between -127 and 0 dBm. |

Command Default The default foreign noise threshold value is -70 dBm.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to set the 802.11a foreign noise threshold for all Cisco lightweight access points to -127 dBm:

```
(Cisco Controller) >config advanced 802.11a profile noise global -127
```

The following example shows how to set the 802.11a foreign noise threshold for AP1 to 0 dBm:

```
(Cisco Controller) >config advanced 802.11a profile noise AP1 0
```

Related Topics

[config advanced 802.11 profile throughput](#), on page 27

[config advanced 802.11 profile foreign](#), on page 25

config advanced 802.11 profile throughput

To set the Cisco lightweight access point data-rate throughput threshold between 1000 and 10000000 bytes per second, use the **config advanced 802.11 profile throughput** command.

config advanced 802.11 { **a** | **b** } **profile throughput** { **global** | *cisco_ap* } *value*

| Syntax Description | | |
|--------------------|--|---|
| a | | Specifies the 802.11a network. |
| b | | Specifies the 802.11b/g network. |
| global | | Configures all 802.11a Cisco lightweight access point specific profiles. |
| <i>cisco_ap</i> | | Cisco lightweight access point name. |
| <i>value</i> | | 802.11a Cisco lightweight access point throughput threshold between 1000 and 10000000 bytes per second. |

Command Default The default Cisco lightweight access point data-rate throughput threshold value is 1,000,000 bytes per second.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to set all Cisco lightweight access point data-rate thresholds to 1000 bytes per second:

```
(Cisco Controller) >config advanced 802.11 profile throughput global 1000
```

The following example shows how to set the AP1 data-rate threshold to 10000000 bytes per second:

```
(Cisco Controller) >config advanced 802.11 profile throughput AP1 10000000
```

Related Topics

[config advanced 802.11 profile foreign](#), on page 25

config advanced 802.11 profile utilization

To set the RF utilization threshold between 0 and 100 percent, use the **config advanced 802.11 profile utilization** command. The operating system generates a trap when this threshold is exceeded.

config advanced 802.11 { **a** | **b** } **profile utilization** { **global** | *cisco_ap* } *percent*

| Syntax Description | | |
|--------------------|--|--|
| a | | Specifies the 802.11a network. |
| b | | Specifies the 802.11b/g network. |
| global | | Configures a global Cisco lightweight access point specific profile. |
| <i>cisco_ap</i> | | Cisco lightweight access point name. |
| <i>percent</i> | | 802.11a RF utilization threshold between 0 and 100 percent. |

Command Default The default RF utilization threshold value is 80 percent.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to set the RF utilization threshold for all Cisco lightweight access points to 0 percent:

```
(Cisco Controller) >config advanced 802.11 profile utilization global 0
```

The following example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
(Cisco Controller) >config advanced 802.11 profile utilization AP1 100
```

Related Topics

[config advanced 802.11 profile throughput](#), on page 27

[config advanced 802.11 profile foreign](#), on page 25

config advanced backup-controller secondary

To configure a secondary backup controller, use the **config advanced backup-controller secondary** command.

config advanced backup-controller secondary *system name IP addr*

| Syntax Description | | |
|--------------------|--------------------|---|
| | <i>system name</i> | Configures primary secondary backup controller. |
| | <i>IP addr</i> | IP address of the backup controller. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines To delete a secondary backup controller entry (IPv4 or IPv6), enter 0.0.0.0 for the controller IP address.

The following example shows how to configure an IPv4 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 10.10.10.10
```

The following example shows how to configure an IPv6 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 2001:9:6:40::623
```

The following example shows how to remove an IPv4 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 0.0.0.0
```

The following example shows how to remove an IPv6 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 0.0.0.0
```

Related Commands **show advanced back-up controller**

config advanced client-handoff

To set the client handoff to occur after a selected number of 802.11 data packet excessive retries, use the **config advanced client-handoff** command.

config advanced client-handoff *num_of_retries*

| | | |
|---------------------------|--|--|
| Syntax Description | <i>num_of_retries</i> | Number of excessive retries before client handoff (from 0 to 255). |
| Command Default | The default value for the number of 802.11 data packet excessive retries is 0. | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

This example shows how to set the client handoff to 100 excessive retries:

```
(Cisco Controller) >config advanced client-handoff 100
```

config advanced dot11-padding

To enable or disable over-the-air frame padding, use the **config advanced dot11-padding** command.

```
config advanced dot11-padding {enable | disable}
```

| Syntax Description | enable | disable |
|--------------------|---|--|
| | Enables the over-the-air frame padding. | Disables the over-the-air frame padding. |

Command Default The default over-the-air frame padding is disabled.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to enable over-the-air frame padding:

```
(Cisco Controller) > config advanced dot11-padding enable
```

| Related Commands |
|--|
| debug dot11 debug dot11 mgmt interface debug dot11 mgmt msg debug dot11 mgmt ssid debug dot11 mgmt state-machine debug dot11 mgmt station show advanced dot11-padding |
| Related Topics config client location-calibration |

config advanced assoc-limit

To configure the rate at which access point radios send association and authentication requests to the controller, use the **config advanced assoc-limit** command.

config advanced assoc-limit { **enable** [*number of associations per interval* | *interval*] | **disable** }

| Syntax Description | | |
|--|--|---|
| enable | | Enables the configuration of the association requests per access point. |
| disable | | Disables the configuration of the association requests per access point. |
| <i>number of associations per interval</i> | | (Optional) Number of association request per access point slot in a given interval. The range is from 1 to 100. |
| <i>interval</i> | | (Optional) Association request limit interval. The range is from 100 to 10000 milliseconds. |

Command Default The default state of the command is disabled state.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines When 200 or more wireless clients try to associate to a controller at the same time, the clients no longer become stuck in the DHCP_REQD state when you use the **config advanced assoc-limit** command to limit association requests from access points.

The following example shows how to configure the number of association requests per access point slot in a given interval of 20 with the association request limit interval of 250:

```
(Cisco Controller) >config advanced assoc-limit enable 20 250
```


config advanced max-1x-sessions

To configure the maximum number of simultaneous 802.1X sessions allowed per access point, use the **config advanced max-1x-sessions** command.

```
config advanced max-1x-sessions no_of_sessions
```

| | | |
|---------------------------|-----------------------|--|
| Syntax Description | <i>no_of_sessions</i> | Number of maximum 802.1x session initiation per AP at a time. The range is from 0 to 255, where 0 indicates unlimited. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to configure the maximum number of simultaneous 802.1X sessions:

```
(Cisco Controller) >config advanced max-1x-sessions 200
```

config advanced probe backoff

To configure the backoff parameters for probe queue in a Cisco AP, use the **config advanced probe backoff** command.

config advanced probe backoff { **enable** | **disable** }

| Syntax Description | |
|--------------------|--|
| enable | To use default backoff parameter value for probe response. |
| disable | To use increased backoff parameters for probe response. |

| Command Default | |
|-----------------|----------|
| | Disabled |

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to use increased backoff parameters for probe response:

```
(Cisco Controller) >config advanced probe backoff enable
```

config advanced probe filter

To configure the filtering of probe requests forwarded from an access point to the controller, use the **config advanced probe filter** command.

```
config advanced probe filter {enable | disable}
```

| | | |
|---------------------------|----------------|---|
| Syntax Description | enable | Enables the filtering of probe requests. |
| | disable | Disables the filtering of probe requests. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to enable the filtering of probe requests forwarded from an access point to the controller:

```
(Cisco Controller) >config advanced probe filter enable
```

config advanced probe limit

To limit the number of probes sent to the WLAN controller per access point per client in a given interval, use the **config advanced probe limit** command.

config advanced probe limit *num_probes interval*

| Syntax Description | | |
|--------------------|-------------------|---|
| | <i>num_probes</i> | Number of probe requests (from 1 to 100) forwarded to the controller per client per access point radio in a given interval. |
| | <i>interval</i> | Probe limit interval (from 100 to 10000 milliseconds). |

Command Default The default number of probe requests is 2. The default interval is 500 milliseconds.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

This example shows how to set the number of probes per access point per client to 5 and the probe interval to 800 milliseconds:

```
(Cisco Controller) >config advanced probe limit 5 800
```

config advanced timers

To configure an advanced system timer, use the **config advanced timers** command.

```
config advanced timers {ap-coverage-report seconds | ap-discovery-timeout discovery-timeout |
ap-fast-heartbeat {local | flexconnect | all} {enable | disable} fast_heartbeat_seconds |
ap-heartbeat-timeout heartbeat_seconds | ap-primary-discovery-timeout primary_discovery_timeout
| ap-primed-join-timeout primed_join_timeout | auth-timeout auth_timeout | pkt-fwd-watchdog
{enable | disable} {watchdog_timer | default} | eap-identity-request-delay
eap_identity_request_delay | eap-timeout eap_timeout}
```

| Syntax | Description |
|-------------------------------|---|
| ap-coverage-report | Configures RRM coverage report interval for all APs. |
| <i>seconds</i> | Configures the ap coverage report interval in seconds. The range is between 60 and 90 seconds. Default is 90 seconds. |
| ap-discovery-timeout | Configures the Cisco lightweight access point discovery timeout value. |
| <i>discovery-timeout</i> | Cisco lightweight access point discovery timeout value, in seconds. The range is from 1 to 10. |
| ap-fast-heartbeat | Configures the fast heartbeat timer, which reduces the amount of time it takes to detect a controller failure in access points. |
| local | Configures the fast heartbeat interval for access points in local mode. |
| flexconnect | Configures the fast heartbeat interval for access points in FlexConnect mode. |
| all | Configures the fast heartbeat interval for all the access points. |
| enable | Enables the fast heartbeat interval. |
| disable | Disables the fast heartbeat interval. |
| <i>fast_heartbeat_seconds</i> | Small heartbeat interval, which reduces the amount of time it takes to detect a controller failure, in seconds. The range is from 1 to 10. |
| ap-heartbeat-timeout | Configures Cisco lightweight access point heartbeat timeout value. |
| <i>heartbeat_seconds</i> | Configures the Cisco lightweight access point heartbeat timeout value, in seconds. The range is from 1 to 30. This value should be at least three times larger than the fast heartbeat timer. |

| | |
|-------------------------------------|--|
| ap-primary-discovery-timeout | Configures the access point primary discovery request timer. |
| <i>primary_discovery_timeout</i> | Access point primary discovery request time, in seconds. The range is from 30 to 3600. |
| ap-primed-join-timeout | Configures the access point primed discovery timeout value. |
| <i>primed_join_timeout</i> | Access point primed discovery timeout value, in seconds. The range is from 120 to 43200. |
| auth-timeout | Configures the authentication timeout. |
| <i>auth_timeout</i> | Authentication response timeout value, in seconds. The range is from 10 to 600. |
| pkt-fwd-watchdog | Configures the packet forwarding watchdog timer to protect from fastpath deadlock. |
| <i>watchdog_timer</i> | Packet forwarding watchdog timer, in seconds. The range is from 60 to 300. |
| default | Configures the watchdog timer to the default value of 240 seconds. |
| eap-identity-request-delay | Configures the advanced Extensible Authentication Protocol (EAP) identity request delay, in seconds. |
| <i>eap_identity_request_delay</i> | Advanced EAP identity request delay, in seconds. The range is from 0 to 10. |
| eap-timeout | Configures the EAP expiration timeout. |
| <i>eap_timeout</i> | EAP timeout value, in seconds. The range is from 8 to 120. |

Command Default

- The default access point discovery timeout is 10 seconds.
- The default access point heartbeat timeout is 30 seconds.
- The default access point primary discovery request timer is 120 seconds.
- The default authentication timeout is 10 seconds.
- The default packet forwarding watchdog timer is 240 seconds.

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

Usage Guidelines

The Cisco lightweight access point discovery timeout indicates how often a Cisco WLC attempts to discover unconnected Cisco lightweight access points.

The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keepalive signal to the Cisco Wireless LAN Controller.

The following example shows how to configure an access point discovery timeout with a timeout value of 20:

```
(Cisco Controller) >config advanced timers ap-discovery-timeout 20
```

The following example shows how to enable the fast heartbeat interval for an access point in FlexConnect mode:

```
(Cisco Controller) >config advanced timers ap-fast-heartbeat flexconnect enable 8
```

The following example shows how to configure the authentication timeout to 20 seconds:

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config ap

To configure a Cisco lightweight access point or to add or delete a third-party (foreign) access point, use the **config ap** command.

```
config ap {{enable | disable} cisco_ap | {add | delete} MAC port {enable | disable} IP_address}
```

| Syntax Description | | |
|--------------------|--|------------------------------|
| enable | Enables the Cisco lightweight access point. | |
| disable | Disables the Cisco lightweight access point. | |
| <i>cisco_ap</i> | Name of the Cisco lightweight access point. | |
| add | Adds foreign access points. | |
| delete | Deletes foreign access points. | |
| <i>MAC</i> | MAC address of a foreign access point. | |
| <i>port</i> | Port number through which the foreign access point can be reached. | |
| <i>IP_address</i> | IP address of the foreign access point. | |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to disable lightweight access point AP1:

```
(Cisco Controller) >config ap disable AP1
```

The following example shows how to add a foreign access point with MAC address 12:12:12:12:12:12 and IP address 192.12.12.1 from port 2033:

```
(Cisco Controller) >config ap add 12:12:12:12:12:12 2033 enable 192.12.12.1
```


config ap cdp

To configure the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **config ap cdp** command.

config ap cdp {enable | disable | interface {ethernet *interface_number* | slot *slot_id*}} {*cisco_ap* | all}

| Syntax Description | | |
|-------------------------|--|--|
| enable | | Enables CDP on an access point. |
| disable | | Disables CDP on an access point. |
| interface | | Configures CDP in a specific interface. |
| ethernet | | Configures CDP for an ethernet interface. |
| <i>interface_number</i> | | Ethernet interface number between 0 and 3. |
| slot | | Configures CDP for a radio interface. |
| <i>slot_id</i> | | Slot number between 0 and 3. |
| <i>cisco_ap</i> | | Name of a Cisco lightweight access point. |
| all | | Specifies all access points. |



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

Command Default Enabled on radio interfaces of mesh APs and disabled on radio interfaces of non-mesh APs. Enabled on Ethernet interfaces of all APs.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines The **config ap cdp disable all** command disables CDP on all access points that are joined to the controller and all access points that join in the future. CDP remains disabled on both current and future access points even after the controller or access point reboots. To enable CDP, enter the **config ap cdp enable all** command.



Note CDP over Ethernet/radio interfaces is available only when CDP is enabled. After you enable CDP on all access points joined to the controller, you may disable and then reenabling CDP on individual access points using the **config ap cdp {enable | disable} cisco_ap command**. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.

The following example shows how to enable CDP on all access points:

```
(Cisco Controller) >config ap cdp enable all
```

The following example shows how to disable CDP on ap02 access point:

```
(Cisco Controller) >config ap cdp disable ap02
```

The following example shows how to enable CDP for Ethernet interface number 2 on all access points:

```
(Cisco Controller) >config ap cdp ethernet 2 enable all
```

config ap core-dump

To configure a Cisco lightweight access point's memory core dump, use the **config ap core-dump** command.

```
config ap core-dump { disable | enable tftp_server_ipaddress filename { compress | uncompress }
{ cisco_ap | all }
```

| Syntax Description | | |
|------------------------------|--|--|
| enable | | Enables the Cisco lightweight access point's memory core dump setting. |
| disable | | Disables the Cisco lightweight access point's memory core dump setting. |
| <i>tftp_server_ipaddress</i> | | IP address of the TFTP server to which the access point sends core dump files. |
| <i>filename</i> | | Name that the access point uses to label the core file. |
| compress | | Compresses the core dump file. |
| uncompress | | Uncompresses the core dump file. |
| <i>cisco_ap</i> | | Name of a Cisco lightweight access point. |
| all | | Specifies all access points. |



Note If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines The access point must be able to reach the TFTP server. This command is applicable for both IPv4 and IPv6 addresses.

The following example shows how to configure and compress the core dump file:

```
(Cisco Controller) >config ap core-dump enable 209.165.200.225 log compress AP02
```

config ap crash-file clear-all

To delete all crash and radio core dump files, use the **config ap crash-file clear-all** command.

config ap crash-file clear-all

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to delete all crash files:

```
(Cisco Controller) >config ap crash-file clear-all
```

config ap crash-file delete

To delete a single crash or radio core dump file, use the **config ap crash-file delete** command.

config ap crash-file delete *filename*

| | | |
|---------------------------|-----------------|------------------------------|
| Syntax Description | <i>filename</i> | Name of the file to delete. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to delete crash file 1:

```
(Cisco Controller) >config ap crash-file delete crash_file_1
```

config ap crash-file get-crash-file

To collect the latest crash data for a Cisco lightweight access point, use the **config ap crash-file get-crash-file** command.

config ap crash-file get-crash-file *cisco_ap*

| | | |
|---------------------------|--|---|
| Syntax Description | <i>cisco_ap</i> | Name of the Cisco lightweight access point. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |
| Usage Guidelines | Use the transfer upload datatype command to transfer the collected data to the Cisco wireless LAN controller. | |

The following example shows how to collect the latest crash data for access point AP3:

```
(Cisco Controller) >config ap crash-file get-crash-file AP3
```

config ap crash-file get-radio-core-dump

To get a Cisco lightweight access point's radio core dump, use the **config ap crash-file get-radio-core-dump** command.

```
config ap crash-file get-radio-core-dump slot_id cisco_ap
```

| | | |
|---------------------------|-----------------|---|
| Syntax Description | <i>slot_id</i> | Slot ID (either 0 or 1). |
| | <i>cisco_ap</i> | Name of a Cisco lightweight access point. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to collect the radio core dump for access point AP02 and slot 0:

```
(Cisco Controller) >config ap crash-file get-radio-core-dump 0 AP02
```

config ap ethernet tag

To configure VLAN tagging of the Control and Provisioning of Wireless Access Points protocol (CAPWAP) packets, use the **config ap ethernet tag** command.

```
config ap ethernet tag {id vlan_id | disable} {cisco_ap | all}
```

| Syntax Description | id | Specifies the VLAN id. |
|--------------------|-----------------|---|
| | <i>vlan_id</i> | ID of the trunk VLAN. |
| | disable | Disables the VLAN tag feature. When you disable VLAN tagging, the access point untags the CAPWAP packets. |
| | <i>cisco_ap</i> | Name of the Cisco AP. |
| | all | Configures VLAN tagging on all the Cisco access points. |

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines

After you configure VLAN tagging, the configuration comes into effect only after the access point reboots. You cannot configure VLAN tagging on mesh access points.

If the access point is unable to route traffic or reach the controller using the specified trunk VLAN, it falls back to the untagged configuration. If the access point joins the controller using this fallback configuration, the controller sends a trap to a trap server such as the Cisco Prime Infrastructure, which indicates the failure of the trunk VLAN. In this scenario, the "Failover to untagged" message appears in show command output.


The following example shows how to configure VLAN tagging on a trunk VLAN:

```
(Cisco Controller) >config ap ethernet tag 6 AP1
```


config ap image swap

To swap an access point's primary and backup images, use the **config ap image swap** command.

config ap image swap { *cisco_ap* | **all** }

| Syntax Description | | |
|------------------------|---|---|
| | <i>cisco_ap</i> | Name of a Cisco lightweight access point. |
| | all | Specifies all access points to interchange the boot images. |
| |  | |
| Note | If an AP itself is configured with the keyword all , the all access points case takes precedence over the AP that is with the keyword all . | |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to swap an access point's primary and secondary images:

```
(Cisco Controller) >config ap image swap all
```

config ap led-state

To configure the LED state of an access point or to configure the flashing of LEDs, use the **config ap led-state** command.

```
config ap led-state {enable | disable} {cisco_ap | all}
```

```
config ap led-state flash {seconds | indefinite | disable} {cisco_ap | dual-band}
```

| Syntax Description | | |
|--------------------|--|--|
| enable | | Enables the LED state of an access point. |
| disable | | Disables the LED state of an access point. |
| <i>cisco_ap</i> | | Name of a Cisco lightweight access point. |
| flash | | Configure the flashing of LEDs for an access point. |
| <i>seconds</i> | | Duration that the LEDs have to flash. The range is from 1 to 3600 seconds. |
| indefinite | | Configures indefinite flashing of the access point's LED. |
| dual-band | | Configures the LED state for all dual-band access points. |

Usage Guidelines



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

LEDs on access points with dual-band radio module will flash green and blue when you execute the led state flash command.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to enable the LED state for an access point:

```
(Cisco Controller) >config ap led-state enable AP02
```

The following example shows how to enable the flashing of LEDs for dual-band access points:

```
(Cisco Controller) >config ap led-state flash 20 dual-band
```

config ap location

To modify the descriptive location of a Cisco lightweight access point, use the **config ap location** command.

config ap location *location cisco_ap*

| Syntax Description | | |
|--------------------|-----------------|---|
| | <i>location</i> | Location name of the access point (enclosed by double quotation marks). |
| | <i>cisco_ap</i> | Name of the Cisco lightweight access point. |

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines The Cisco lightweight access point must be disabled before changing this parameter.

The following example shows how to configure the descriptive location for access point AP1:

```
(Cisco Controller) >config ap location "Building 1" AP1
```

config ap logging syslog level

To set the severity level for filtering syslog messages for a particular access point or for all access points, use the **config ap logging syslog level** command.

config ap logging syslog level *severity_level* { *cisco_ap* | **all** }

Syntax Description

severity_level

Severity levels are as follows:

- emergencies—Severity level 0
- alerts—Severity level 1
- critical—Severity level 2
- errors—Severity level 3
- warnings—Severity level 4
- notifications—Severity level 5
- informational—Severity level 6
- debugging—Severity level 7

cisco_ap

Cisco access point.

all

Specifies all access points.



Note

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

Command Default

None

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

Usage Guidelines

If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the access point. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the access point.

This example shows how to set the severity for filtering syslog messages to 3:

```
(Cisco Controller) >config ap logging syslog level 3
```

config ap mgmtuser add

To configure username, password, and secret password for AP management, use the **config ap mgmtuser add** command.

```
config ap mgmtuser add username AP_username password AP_password secret secret { all | cisco_ap }
```

| Syntax | Description |
|--------------------|---|
| username | Configures the username for AP management. |
| <i>AP_username</i> | Management username. |
| password | Configures the password for AP management. |
| <i>AP_password</i> | AP management password. |
| secret | Configures the secret password for privileged AP management. |
| <i>secret</i> | AP management secret password. |
| all | Applies configuration to every AP that does not have a specific username. |
| <i>cisco_ap</i> | Cisco access point. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines

The following requirements are enforced on the password:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain management username or reverse of username.
- The password should not contain words like Cisco, oscie, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting \$ for s.

The following requirement is enforced on the secret password:

- The secret password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, or special characters.

The following example shows how to add a username, password, and secret password for AP management:

```
(Cisco Controller) > config ap mgmtuser add username acd password Arc_1234 secret Mid_45  
all
```

config ap mgmtuser delete

To force a specific access point to use the controller's global credentials, use the **config ap mgmtuser delete** command.

config ap mgmtuser delete *cisco_ap*

| | | |
|---------------------------|-----------------|------------------------------|
| Syntax Description | <i>cisco_ap</i> | Access point. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to delete the credentials of an access point:

```
(Cisco Controller) > config ap mgmtuser delete cisco_ap1
```

config ap monitor-mode

To configure Cisco lightweight access point channel optimization, use the **config ap monitor-mode** command.

```
config ap monitor-mode {802.11b fast-channel | no-optimization | tracking-opt | wips-optimized}
cisco_ap
```

| Syntax Description | | |
|--------------------|-----------------------------|---|
| | 802.11b fast-channel | Configures 802.11b scanning channels for a monitor-mode access point. |
| | no-optimization | Specifies no channel scanning optimization for the access point. |
| | tracking-opt | Enables tracking optimized channel scanning for the access point. |
| | wips-optimized | Enables wIPS optimized channel scanning for the access point. |
| | <i>cisco_ap</i> | Name of the Cisco lightweight access point. |

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to configure a Cisco wireless intrusion prevention system (wIPS) monitor mode on access point AP01:

```
(Cisco Controller) > config ap monitor-mode wips-optimized AP01
```


config ap name

To modify the name of a Cisco lightweight access point, use the **config ap name** command.

config ap name *new_name old_name*

| | | |
|---------------------------|-----------------|--|
| Syntax Description | <i>new_name</i> | Desired Cisco lightweight access point name. |
| | <i>old_name</i> | Current Cisco lightweight access point name. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to modify the name of access point AP1 to AP2:

```
(Cisco Controller) > config ap name AP1 AP2
```

config ap packet-dump

To configure the Packet Capture parameters on access points, use the **config ap packet-dump** command.

```
config ap packet-dump {buffer-size Size_in_KB | capture-time Time_in_Min | ftp serverip IP_addr
path path username username password password | start MAC_address Cisco_AP | stop | truncate
Length_in_Bytes}
config ap packet-dump classifier {{arp | broadcast | control | data | dot1x | iapp | ip |
management | multicast } {enable | disable} | tcp {enable | disable} | port TCP_Port {enable
| disable}} | udp {enable | disable} | port UDP_Port {enable | disable}}}
```

| Syntax | Description |
|---------------------------------|---|
| buffer-size | Configures the buffer size for Packet Capture in the access point. |
| <i>Size_in_KB</i> | Size of the buffer. The range is from 1024 to 4096 KB. |
| capture-time | Configures the timer value for Packet Capture. |
| <i>Time_in_Min</i> | Timer value for Packet Capture. The range is from 1 to 60 minutes. |
| ftp | Configures FTP parameters for Packet Capture. |
| serverip | Configures the FTP server. |
| <i>IP_addr</i> | IP address of the FTP server. |
| path <i>path</i> | Configures FTP server path. |
| username <i>user_ID</i> | Configures the username for the FTP server. |
| password <i>password</i> | Configures the password for the FTP server. |
| start | Starts Packet Capture from the access point. |
| <i>MAC_address</i> | Client MAC Address for Packet Capture. |
| <i>Cisco_AP</i> | Name of the Cisco access point. |
| stop | Stops Packet Capture from the access point. |
| truncate | Truncates the packet to the specified length during Packet Capture. |

| | |
|------------------------|---|
| <i>Length_in_Bytes</i> | Length of the packet after truncation. The range is from 20 to 1500. |
| classifier | Configures the classifier information for Packet Capture. You can specify the type of packets that needs to be captured. |
| arp | Captures ARP packets. |
| enable | Enables capture of ARP, broadcast, 802.11 control, 802.11 data, dot1x, Inter Access Point Protocol (IAPP), IP, 802.11 management, or multicast packets. |
| disable | Disables capture of ARP, broadcast, 802.11 control, 802.11 data, dot1x, IAPP, IP, 802.11 management, or multicast packets. |
| broadcast | Captures broadcast packets. |
| control | Captures 802.11 control packets. |
| data | Captures 802.11 data packets. |
| dot1x | Captures dot1x packets. |
| iapp | Captures IAPP packets. |
| ip | Captures IP packets. |
| management | Captures 802.11 management packets. |
| multicast | Captures multicast packets. |
| tcp | Captures TCP packets. |
| <i>TCP_Port</i> | TCP port number. The range is from 1 to 65535. |
| udp | Captures UDP packets. |
| <i>UDP_Port</i> | UDP port number. The range is from 1 to 65535. |
| ftp | Configures FTP parameters for Packet Capture. |
| <i>server_ip</i> | FTP server IP address. |

Command Default The default buffer size is 2 MB. The default capture time is 10 minutes.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines Packet Capture does not work during intercontroller roaming.

The controller does not capture packets created in the radio firmware and sent out of the access point, such as a beacon or probe response. Only packets that flow through the Radio driver in the Tx path will be captured.

Use the command **config ap packet-dump start** to start the Packet Capture from the access point. When you start Packet Capture, the controller sends a Control and Provisioning of Wireless Access Points protocol (CAPWAP) message to the access point to which the client is associated and captures packets. You must configure the FTP server and ensure that the client is associated to the access point before you start Packet Capture. If the client is not associated to the access point, you must specify the name of the access point.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to start Packet Capture from an access point:

```
(Cisco Controller) >config ap packet-dump start 00:0d:28:f4:c0:45 AP1
```

The following example shows how to capture 802.11 control packets from an access point:

```
(Cisco Controller) >config ap packet-dump classifier control enable
```

config ap port

To configure the port for a foreign access point, use the **config ap port** command.

config ap port *MAC port*

| | | |
|---------------------------|----------------|---|
| Syntax Description | <i>MAC</i> | Foreign access point MAC address. |
| | <i>port</i> | Port number for accessing the foreign access point. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to configure the port for a foreign access point MAC address:

```
(Cisco Controller) > config ap port 12:12:12:12:12:12 20
```

config ap power injector

To configure the power injector state for an access point, use the **config ap power injector** command.

```
config ap power injector {enable | disable} {cisco_ap | all} {installed | override |
switch_MAC}
```

| Syntax | Description |
|-------------------|---|
| enable | Enables the power injector state for an access point. |
| disable | Disables the power injector state for an access point. |
| <i>cisco_ap</i> | Name of the Cisco lightweight access point. |
| all | Specifies all Cisco lightweight access points connected to the controller. |
| installed | Detects the MAC address of the current switch port that has a power injector. |
| override | Overrides the safety checks and assumes a power injector is always installed. |
| <i>switch_MAC</i> | MAC address of the switch port with an installed power injector. |



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

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to enable the power injector state for all access points:

```
(Cisco Controller) > config ap power injector enable all 12:12:12:12:12:12
```

config ap power pre-standard

To enable or disable the inline power Cisco pre-standard switch state for an access point, use the **config ap power pre-standard** command.

```
config ap power pre-standard {enable | disable} cisco_ap
```

| Syntax Description | enable | disable | cisco_ap |
|--------------------|---|--|---|
| | Enables the inline power Cisco pre-standard switch state for an access point. | Disables the inline power Cisco pre-standard switch state for an access point. | Name of the Cisco lightweight access point. |
| Command Default | Disabled. | | |
| Command History | Release | Modification | |
| | 8.3 | This command was introduced. | |

The following example shows how to enable the inline power Cisco pre-standard switch state for access point AP02:

```
(Cisco Controller) > config ap power pre-standard enable AP02
```

config ap preferred-mode

To configure the preferred mode, use the **config ap preferred-mode** command.

config ap preferred-mode { **ipv4** | **ipv6** | **any** } { *AP_name* | *Ap-group_name* | *all* }

Syntax Description

| | |
|----------------------|---|
| ipv4 | Configures IPv4 as the preferred mode |
| ipv6 | Configures IPv6 as the preferred mode |
| any | Configures any as the preferred mode |
| <i>AP_name</i> | Configures the preferred mode to the AP |
| <i>Ap-group_name</i> | Configures the preferred mode to the AP group members |
| <i>all</i> | Configures the preferred mode to all the APs |

Command Default

None

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

Example

The following example shows how to configure IPv6 as the preferred mode to lightweight access point AP1

```
(Cisco Controller) >config ap preferred-mode ipv6 AP1
```


config ap primary-base

To set the Cisco lightweight access point primary Cisco WLC, use the **config ap primary-base** command.

config ap primary-base *controller_name* *Cisco_AP* [*controller_ip_address*]

| Syntax Description | | |
|------------------------------|-------------|--|
| <i>controller_name</i> | | Name of the Cisco WLC. |
| <i>Cisco_AP</i> | | Cisco lightweight access point name. |
| <i>controller_ip_address</i> | | (Optional) If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller. |
| | Note | For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines The Cisco lightweight access point associates with this Cisco WLC for all network operations and in the event of a hardware reset.

OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to set an access point primary Cisco WLC IPv4 address for an Cisco AP:

```
(Cisco Controller) > config ap primary-base SW_1 AP2 10.0.0.0
```

The following example shows how to set an access point primary Cisco WLC IPv6 address for an Cisco AP:

```
(Cisco Controller) > config ap primary-base SW_1 AP2 2001:DB8:0:1::1
```

Related Commands **show ap config general**

config ap reporting-period

To reset a Cisco lightweight access point, use the **config ap reporting-period** command.

config ap reporting-period *period*

| | | |
|---------------------------|----------------|--|
| Syntax Description | <i>period</i> | Time period in seconds between 10 and 120. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to reset an access point reporting period to 120 seconds:

```
> config ap reporting-period 120
```

config ap reset

To reset a Cisco lightweight access point, use the **config ap reset** command.

```
config ap reset cisco_ap
```

| | | |
|---------------------------|-----------------|--------------------------------------|
| Syntax Description | <i>cisco_ap</i> | Cisco lightweight access point name. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to reset an access point:

```
(Cisco Controller) > config ap reset AP2
```

config ap retransmit interval

To configure the access point control packet retransmission interval, use the **config ap retransmit interval** command.

config ap retransmit interval *seconds* {**all** | *cisco_ap*}

| Syntax Description | <i>seconds</i> | AP control packet retransmission timeout between 2 and 5 seconds. |
|--------------------|-----------------|---|
| | all | Specifies all access points. |
| | <i>cisco_ap</i> | Cisco lightweight access point name. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to configure the retransmission interval for all access points globally:

```
(Cisco Controller) > config ap retransmit interval 4 all
```

config ap retransmit count

To configure the access point control packet retransmission count, use the **config ap retransmit count** command.

```
config ap retransmit count count {all | cisco_ap}
```

| Syntax Description | | |
|--------------------|---|------------------------------|
| <i>count</i> | Number of times control packet will be retransmitted. The range is from 3 to 8. | |
| all | Specifies all access points. | |
| <i>cisco_ap</i> | Cisco lightweight access point name. | |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to configure the retransmission retry count for a specific access point:

```
(Cisco Controller) > config ap retransmit count 6 cisco_ap
```

config ap sniff

To enable or disable sniffing on an access point, use the **config ap sniff** command.

```
config ap sniff {802.11a | 802.11b} {enable channel server_ip | disable} cisco_ap
```

| Syntax Description | | |
|--------------------|--|---|
| 802.11a | | Specifies the 802.11a network. |
| 802.11b | | Specifies the 802.11b network. |
| enable | | Enables sniffing on an access point. |
| <i>channel</i> | | Channel to be sniffed. |
| <i>server_ip</i> | | IP address of the remote machine running Omnippeek, Airopeek, AirMagnet, or Wireshark software. |
| disable | | Disables sniffing on an access point. |
| <i>cisco_ap</i> | | Access point configured as the sniffer. |

Command Default Channel 36.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines When the sniffer feature is enabled on an access point, it starts sniffing the signal on the given channel. It captures and forwards all the packets to the remote computer that runs Omnippeek, Airopeek, AirMagnet, or Wireshark software. It includes information on the timestamp, signal strength, packet size and so on.

Before an access point can act as a sniffer, a remote computer that runs one of the listed packet analyzers must be set up so that it can receive packets sent by the access point. After the Airopeek installation, copy the following .dll files to the location where airopeek is installed:

- socket.dll file to the Plug-ins folder (for example, C:\Program Files\WildPackets\AiroPeek\Plugins)
- socketres.dll file to the PluginRes folder (for example, C:\Program Files\WildPackets\AiroPeek\1033\PluginRes)

The following example shows how to enable the sniffing on the 802.11a an access point from the primary Cisco WLC:

```
(Cisco Controller) > config ap sniff 80211a enable 23 11.22.44.55 AP01
```

config ap ssh

To enable Secure Shell (SSH) connectivity on an access point, use the **config ap ssh** command.

```
config ap ssh {enable | disable | default} cisco_ap | all
```

| Syntax Description | enable | enable |
|--------------------|----------|---|
| | enable | Enables the SSH connectivity on an access point. |
| | disable | Disables the SSH connectivity on an access point. |
| | default | Replaces the specific SSH configuration of an access point with the global SSH configuration. |
| | cisco_ap | Cisco access point name. |
| | all | All access points. |

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operation and in the event of a hardware reset.

The following example shows how to enable SSH connectivity on access point Cisco_ap2:

```
> config ap ssh enable cisco_ap2
```

config ap static-ip

To configure Static IP address settings on Cisco lightweight access point , use the **config ap static-ip** command.

```
config ap static-ip { enable Cisco_AP AP_IP_addr IP_netmask /prefix_length gateway | disable
Cisco_AP | add { domain { Cisco_AP | all } domain_name | nameserver { Cisco_AP | all }
nameserver-ip } | delete { domain | nameserver } { Cisco_AP | all }
```

Syntax Description

| | |
|---------------------------------|---|
| enable | Enables the Cisco lightweight access point static IP address. |
| disable | Disables the Cisco lightweight access point static IP address. The access point uses DHCP to get the IP address. |
| <i>Cisco_AP</i> | Cisco lightweight access point name. |
| <i>AP_IP_addr</i> | Cisco lightweight access point IP address |
| <i>IP_netmask/prefix_length</i> | Cisco lightweight access point network mask. |
| <i>gateway</i> | IP address of the Cisco lightweight access point gateway. |
| add | Adds a domain or DNS server. |
| domain | Specifies the domain to which a specific access point or all access points belong. |
| all | Specifies all access points. |
| <i>domain_name</i> | Specifies a domain name. |
| nameserver | Specifies a DNS server so that a specific access point or all access points can discover the controller using DNS resolution. |
| <i>nameserver-ip</i> | DNS server IP address. |
| delete | Deletes a domain or DNS server. |



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

Command Default

None

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

Usage Guidelines

An access point cannot discover the controller using Domain Name System (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs.

After you enter the IPv6 address, Prefix-length and IPv6 gateway address, the CAPWAP tunnel will restart for access point. Changing the AP's IP address will cause the AP to disjoin. After the access point rejoins the controller, you can enter the domain and IPv6 DNS server information.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure static IP address on an access point:

```
(Cisco Controller) >config ap static-ip enable AP2 209.165.200.225 255.255.255.0  
209.165.200.254
```

The following example shows how to configure static IPv6 address on an access point:

```
(Cisco Controller) > config ap static-ip enable AP2 2001:DB8:0:1::1
```

Related Commands

show ap config general

config ap stats-timer

To set the time in seconds that the Cisco lightweight access point sends its DOT11 statistics to the Cisco wireless LAN controller, use the **config ap stats-timer** command.

config ap stats-timer *period cisco_ap*

| | | |
|---------------------------|--|---|
| Syntax Description | <i>period</i> | Time in seconds from 0 to 65535. A zero value disables the timer. |
| | <i>cisco_ap</i> | Cisco lightweight access point name. |
| Command Default | The default value is 0 (disabled state). | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

Usage Guidelines A value of 0 (zero) means that the Cisco lightweight access point does not send any DOT11 statistics. The acceptable range for the timer is from 0 to 65535 seconds, and the Cisco lightweight access point must be disabled to set this value.

The following example shows how to set the stats timer to 600 seconds for access point AP2:

```
(Cisco Controller) > config ap stats-timer 600 AP2
```

config ap syslog host global

To configure a global syslog server for all access points that join the controller, use the **config ap syslog host global** command.

config ap syslog host global *ip_address*

| | | |
|---------------------------|--|---|
| Syntax Description | <i>ip_address</i> | IPv4/IPv6 address of the syslog server. |
| Command Default | The default value of the IPv4 address of the syslog server is 255.255.255.255. | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

Usage Guidelines

By default, the global syslog server IP address for all access points is 255.255.255.255. Make sure that the access points can reach the subnet on which the syslog server resides before configuring the syslog server on the controller. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure a global syslog server, using IPv4 address, for all access points:

```
(Cisco Controller) > config ap syslog host global 255.255.255.255
```

The following example shows how to configure a global syslog server, using IPv6 address, for all access points:

```
(Cisco Controller) > config ap syslog host global 2001:9:10:56::100
```

config ap syslog host specific

To configure a syslog server for a specific access point, use the **config ap syslog host specific** command.

config ap syslog host specific *ap_name* *ip_address*

| Syntax Description | | |
|--------------------|-------------------|---|
| | <i>ap_name</i> | Cisco lightweight access point. |
| | <i>ip_address</i> | IPv4/IPv6 address of the syslog server. |

Command Default The default value of the syslog server IP address is 0.0.0.0.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines By default, the syslog server IP address for each access point is 0.0.0.0, indicating that it is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure a syslog server:

```
(Cisco Controller) >config ap syslog host specific 0.0.0.0
```

The following example shows how to configure a syslog server for a specific AP, using IPv6 address:

```
(Cisco Controller) > config ap syslog host specific AP3600 2001:9:10:56::100
```

config ap tcp-mss-adjust

To enable or disable the TCP maximum segment size (MSS) on a particular access point or on all access points, use the **config ap tcp-mss-adjust** command.

config ap tcp-mss-adjust {enable | disable} {cisco_ap | all} size

| Syntax Description | | |
|--------------------|--|--|
| enable | | Enables the TCP maximum segment size on an access point. |
| disable | | Disables the TCP maximum segment size on an access point. |
| <i>cisco_ap</i> | | Cisco access point name. |
| all | | Specifies all access points. |
| <i>size</i> | | Maximum segment size. <ul style="list-style-type: none"> • IPv4—Specify a value between 536 and 1363. • IPv6—Specify a value between 1220 and 1331. <p>Note Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP.</p> |



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

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines When you enable this feature, the access point checks for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

This example shows how to enable the TCP MSS on access point `cisco_ap1` with a segment size of 1200 bytes:

```
(Cisco Controller) > config ap tcp-mss-adjust enable cisco_ap1 1200
```

config ap telnet

To enable Telnet connectivity on an access point, use the **config ap telnet** command.

config ap telnet {**enable** | **disable** | **default**} *cisco_ap* | *all*

Syntax Description

| | |
|-----------------|---|
| enable | Enables the Telnet connectivity on an access point. |
| disable | Disables the Telnet connectivity on an access point. |
| default | Replaces the specific Telnet configuration of an access point with the global Telnet configuration. |
| <i>cisco_ap</i> | Cisco access point name. |
| <i>all</i> | All access points. |

Command Default

None

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

Usage Guidelines

- The Cisco lightweight access point associates with this Cisco WLC for all network operation and in the event of a hardware reset.
- Telnet is not supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs.

The following example shows how to enable Telnet connectivity on access point *cisco_ap1*:

```
(Cisco Controller) >config ap telnet enable cisco_ap1
```

The following example shows how to disable Telnet connectivity on access point *cisco_ap1*:

```
(Cisco Controller) > config ap telnet disable cisco_ap1
```

config ap timezone

To configure the timezone for Cisco access points, use the **config ap timezone** command.

```
config ap timezone{enable{use-controller{ cisco_ap| all } | delta{cisco_ap| all {  
remote_timezone_offset_hour remote_timezone_offset_minute } } | disable {cisco_ap|all} | default
```

| | |
|--------------------------------------|--|
| enable | Enables time zone configuration for Cisco access points. |
| disable | Disables time zone configuration for Cisco access points. |
| default | Replaces the specific time zone configuration with global time zone configuration. |
| use-controller | Applies the time zone configuration of the current controller. |
| delta | Configures time zone specific to the access point. |
| <i>cisco_ap</i> | Name of the access point to which the command applies. |
| all | Applies controller time zone configuration in all Cisco access points. |
| <i>remote_timezone_offset_hour</i> | The hour offset from the GMT. The valid range for this variable is between -23 and 23 |
| <i>remote_timezone_offset_minute</i> | The minute offset from the GMT. The valid range for this variable is between 0 and 60. |

Example

The following example shows how to configure Pacific Standard Time on a Cisco Access Point:

```
config ap timezoneenable delta stark12 -08 00
```

config ap username

To assign a username and password to access either a specific access point or all access points, use the **config ap username** command.

```
config ap username user_id password passwd [all | ap_name]
```

| Syntax Description | | |
|--------------------|---|------------------------------|
| <i>user_id</i> | Administrator username. | |
| <i>passwd</i> | Administrator password. | |
| all | (Optional) Specifies all access points. | |
| <i>ap_name</i> | Name of a specific access point. | |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to assign a username and password to a specific access point:

```
(Cisco Controller) > config ap username jack password blue 1a204
```

The following example shows how to assign the same username and password to a all access points:

```
(Cisco Controller) > config ap username jack password blue all
```


config ap venue

To configure the venue information for 802.11u network on an access point, use the **config ap venue** command.

config ap venue { **add** *venue_name* *venue-group* *venue-type* *lang-code* *cisco-ap* | **delete** }

| Syntax Description | add | Description |
|--------------------|--------------------|---|
| | <i>venue_name</i> | Venue name. |
| | <i>venue_group</i> | Venue group category. See the table below for details on venue group mappings. |
| | <i>venue_type</i> | Venue type. This value depends on the venue-group specified. See the table below for venue group mappings. |
| | <i>lang_code</i> | Language used. An ISO-14962-1997 encoded string that defines the language. This string is a three character language code. Enter the first three letters of the language in English (for example, eng for English). |
| | <i>cisco_ap</i> | Name of the access point. |
| | deletes | Deletes venue information. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to set the venue details for an access point named cisco-ap1:

```
(Cisco Controller) > config ap venue add test 11 34 eng cisco-ap1
```

This table lists the different venue types for each venue group.

Table 1: Venue Group Mapping

| Venue Group Name | Value | Venue Type for Group |
|------------------|-------|----------------------|
| UNSPECIFIED | 0 | |

| Venue Group Name | Value | Venue Type for Group |
|------------------|-------|--|
| ASSEMBLY | 1 | <ul style="list-style-type: none"> • 0—UNSPECIFIED ASSEMBLY • 1—ARENA • 2—STADIUM • 3—PASSENGER TERMINAL (E.G., AIRPORT, BUS, FERRY, TRAIN STATION) • 4—AMPHITHEATER • 5—AMUSEMENT PARK • 6—PLACE OF WORSHIP • 7—CONVENTION CENTER • 8—LIBRARY • 9—MUSEUM • 10—RESTAURANT • 11—THEATER • 12—BAR • 13—COFFEE SHOP • 14—ZOO OR AQUARIUM • 15—EMERGENCY COORDINATION CENTER |

| Venue Group Name | Value | Venue Type for Group |
|--------------------|-------|--|
| BUSINESS | 2 | <ul style="list-style-type: none"> • 0—UNSPECIFIED BUSINESS • 1—DOCTOR OR DENTIST OFFICE • 2—BANK • 3—FIRE STATION • 4—POLICE STATION • 6—POST OFFICE • 7—PROFESSIONAL OFFICE • 8—RESEARCH AND DEVELOPMENT FACILITY • 9—ATTORNEY OFFICE |
| EDUCATIONAL | 3 | <ul style="list-style-type: none"> • 0—UNSPECIFIED EDUCATIONAL • 1—SCHOOL, PRIMARY • 2—SCHOOL, SECONDARY • 3—UNIVERSITY OR COLLEGE |
| FACTORY-INDUSTRIAL | 4 | <ul style="list-style-type: none"> • 0—UNSPECIFIED FACTORY AND INDUSTRIAL • 1—FACTORY |
| INSTITUTIONAL | 5 | <ul style="list-style-type: none"> • 0—UNSPECIFIED INSTITUTIONAL • 1—HOSPITAL • 2—LONG-TERM CARE FACILITY (E.G., NURSING HOME, HOSPICE, ETC.) • 3—ALCOHOL AND DRUG RE-HABILITATION CENTER • 4—GROUP HOME • 5—PRISON OR JAIL |

| Venue Group Name | Value | Venue Type for Group |
|------------------|-------|---|
| MERCANTILE | 6 | <ul style="list-style-type: none"> • 0—UNSPECIFIED MERCANTILE • 1—RETAIL STORE • 2—GROCERY MARKET • 3—AUTOMOTIVE SERVICE STATION • 4—SHOPPING MALL • 5—GAS STATION |
| RESIDENTIAL | 7 | <ul style="list-style-type: none"> • 0—UNSPECIFIED RESIDENTIAL • 1—PRIVATE RESIDENCE • 2—HOTEL OR MOTEL • 3—DORMITORY • 4—BOARDING HOUSE |
| STORAGE | 8 | UNSPECIFIED STORAGE |
| UTILITY-MISC | 9 | 0—UNSPECIFIED UTILITY AND MISCELLANEOUS |
| VEHICULAR | 10 | <ul style="list-style-type: none"> • 0—UNSPECIFIED VEHICULAR • 1—AUTOMOBILE OR TRUCK • 2—AIRPLANE • 3—BUS • 4—FERRY • 5—SHIP OR BOAT • 6—TRAIN • 7—MOTOR BIKE |

| Venue Group Name | Value | Venue Type for Group |
|------------------|-------|--|
| OUTDOOR | 11 | <ul style="list-style-type: none">• 0—UNSPECIFIED OUTDOOR• 1—MUNI-MESH NETWORK• 2—CITY PARK• 3—REST AREA• 4—TRAFFIC CONTROL• 5—BUS STOP• 6—KIOSK |

config ap wlan

To enable or disable wireless LAN override for a Cisco lightweight access point radio, use the **config ap wlan** command.

```
config ap wlan {enable | disable} {802.11a | 802.11b} wlan_id cisco_ap
```

| Syntax Description | | |
|--------------------|--|--|
| enable | | Enables the wireless LAN override on an access point. |
| disable | | Disables the wireless LAN override on an access point. |
| 802.11a | | Specifies the 802.11a network. |
| 802.11b | | Specifies the 802.11b network. |
| <i>wlan_id</i> | | Cisco wireless LAN controller ID assigned to a wireless LAN. |
| <i>cisco_ap</i> | | Cisco lightweight access point name. |

| Command Default | |
|-----------------|--|
| None | |

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to enable wireless LAN override on the AP03 802.11a radio:

```
(Cisco Controller) > config ap wlan 802.11a AP03
```

config country

To configure the controller's country code, use the **config country** command.

config country *country_code*

| | | |
|---------------------------|---|--|
| Syntax Description | <i>country_code</i> | Two-letter or three-letter country code. |
| Command Default | <i>us</i> (country code of the United States of America). | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

Usage Guidelines

Cisco WLCs must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.

You can use the **show country** command to display a list of supported countries.

The following example shows how to configure the controller's country code to DE:

```
(Cisco Controller) >config country DE
```

config known ap

To configure a known Cisco lightweight access point, use the **config known ap** command.

```
config known ap {add | alert | delete} MAC
```

| Syntax Description | | |
|--------------------|--|------------------------------|
| add | Adds a new known access point entry. | |
| alert | Generates a trap upon detection of the access point. | |
| delete | Deletes an existing known access point entry. | |
| <i>MAC</i> | MAC address of the known Cisco lightweight access point. | |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to add a new access point entry ac:10:02:72:2f:bf on a known access point:

```
(Cisco Controller) >config known ap add ac:10:02:72:2f:bf 12
```


clear ap config

To clear (reset to the default values) a lightweight access point's configuration settings, use the **clear ap config** command.

clear ap config *ap_name*

| | | |
|---------------------------|---|------------------------------|
| Syntax Description | <i>ap_name</i> | Access point name. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |
| Usage Guidelines | Entering this command does not clear the static IP address of the access point. | |

The following example shows how to clear the access point's configuration settings for the access point named ap1240_322115:

```
(Cisco Controller) >clear ap config ap1240_322115
Clear ap-config will clear ap config and reboot the AP. Are you sure you want continue?
(y/n)
```

clear ap eventlog

To delete the existing event log and create an empty event log file for a specific access point or for all access points joined to the controller, use the **clear ap eventlog** command.

clear ap eventlog {*specific ap_name* | **all**}

| Syntax Description | specific | Specifies a specific access point log file. |
|--------------------|----------------|---|
| | <i>ap_name</i> | Name of the access point for which the event log file is emptied. |
| | all | Deletes the event log for all access points joined to the controller. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to delete the event log for all access points:

```
(Cisco Controller) >clear ap eventlog all
This will clear event log contents for all APs. Do you want continue? (y/n) :y
All AP event log contents have been successfully cleared.
```

clear ap join stats

To clear the join statistics for all access points or for a specific access point, use the **clear ap join stats** command.

```
clear ap join stats {all | ap_mac}
```

| | | |
|---------------------------|----------------|------------------------------|
| Syntax Description | all | Specifies all access points. |
| | <i>ap_mac</i> | Access point MAC address. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to clear the join statistics of all the access points:

```
(Cisco Controller) >clear ap join stats all
```

clear ap tsm

To clear the Traffic Stream Metrics (TSM) statistics of clients associated to an access point, use the **clear ap tsm** command.

```
clear ap tsm {802.11a | 802.11b} cisco_ap all
```

| Syntax Description | |
|--------------------|---|
| 802.11a | Clears 802.11a TSM statistics of clients associated to an access point. |
| 802.11b | Clears 802.11b TSM statistics of clients associated to an access point. |
| <i>cisco_ap</i> | Cisco lightweight access point. |
| all | Clears TSM statistics of clients associated to the access point. |

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to clear 802.11a TSM statistics for all clients of an access point:

```
(Cisco Controller) >clear ap tsm 802.11a AP3600_1 all
```

debug ap

To configure the remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use the **debug ap** command.

debug ap { **enable** | **disable** | **command cmd** } *cisco_ap*

| Syntax | Description |
|-----------------|---|
| enable | <p>Enables the debugging on a lightweight access point.</p> <p>Note The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.</p> |
| disable | <p>Disables the debugging on a lightweight access point.</p> <p>Note The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.</p> |
| command | <p>Specifies that a CLI command is to be executed on the access point.</p> |
| <i>cmd</i> | <p>Command to be executed.</p> <p>Note The command to be executed must be enclosed in double quotes, such as debug ap command "led flash 30" AP03. The output of the command displays only to the controller console and does not send output to a controller Telnet/SSH CLI session.</p> |
| <i>cisco_ap</i> | <p>Name of a Cisco lightweight access point.</p> |

Command Default The remote debugging of Cisco lightweight access points is disabled.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to enable the remote debugging on access point AP01:

```
(Cisco Controller) >debug ap enable AP01
```

The following example shows how to execute the **config ap location** command on access point AP02:

```
(Cisco Controller) >debug ap command "config ap location "Building 1" AP02"
```

The following example shows how to execute the flash LED command on access point AP03:

```
(Cisco Controller) >debug ap command "led flash 30" AP03
```

debug ap enable

To configure the remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use the **debug ap enable** command.

debug ap {**enable** | **disable** | **command cmd**} *cisco_ap*

| Syntax Description | enable | disable | command | cmd | cisco_ap |
|--------------------|---|--------------------------------|---|---|--------------------------------------|
| | Enables the remote debugging. | Disables the remote debugging. | Specifies that a CLI command is to be executed on the access point. | Command to be executed. | Cisco lightweight access point name. |
| | <p>Note The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.</p> | | | <p>Note The command to be executed must be enclosed in double quotes, such as debug ap command "led flash 30" AP03.</p> <p>The output of the command displays only to the controller console and does not send output to a controller Telnet/SSH CLI session.</p> | |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to enable the remote debugging on access point AP01:

```
(Cisco Controller) >debug ap enable AP01
```

The following example shows how to disable the remote debugging on access point AP02:

```
(Cisco Controller) >debug ap disable AP02
```

The following example shows how to execute the flash LED command on access point AP03:

```
(Cisco Controller) >debug ap command "led flash 30" AP03
```

debug ap packet-dump

To configure the debugging of Packet Capture, use the **debug ap packet-dump** command.

debug ap packet-dump { **enable** | **disable** }

| Syntax Description | |
|--------------------|--|
| enable | Enables the debugging of Packet Capture of an access point. |
| disable | Disables the debugging of Packet Capture of an access point. |

Command Default Debugging of Packet Capture is disabled.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines Packet Capture does not work during inter-Cisco WLC roaming.

The Cisco WLC does not capture packets created in the radio firmware and sent out of the access point, such as beacon or probe response. Only packets that flow through the radio driver in the Tx path will be captured.

The following example shows how to enable the debugging of Packet Capture from an access point:

```
(Cisco Controller) >debug ap packet-dump enable
```


debug ap show stats

To debug video messages and statistics of Cisco lightweight access points, use the **debug ap show stats** command.

```
debug ap show stats {802.11a | 802.11b} cisco_ap {tx-queue | packet | load | multicast |
client {client_MAC | video | all} | video metrics}
```

```
debug ap show stats video cisco_ap {multicast mgid mgid_database_number | admission | bandwidth}
```

| Syntax | Description |
|-----------------------------|---|
| 802.11a | Specifies the 802.11a network. |
| 802.11b | Specifies the 802.11b/g network. |
| <i>cisco_ap</i> | Cisco lightweight access point name. |
| tx-queue | Displays the transmit queue traffic statistics of the AP. |
| packet | Displays the packet statistics of the AP. |
| load | Displays the QoS Basic Service Set (QBSS) and other statistics of the AP. |
| multicast | Displays the multicast supported rate statistics of the AP. |
| client | Displays the specified client metric statistics. |
| <i>client_MAC</i> | MAC address of the client. |
| video | Displays video statistics of all clients on the AP. |
| all | Displays statistics of all clients on the AP. |
| video metrics | Displays the video metric statistics. |
| mgid | Displays detailed multicast information for a single multicast group ID (MGID). |
| <i>mgid_database_number</i> | Layer 2 MGID database number. |
| admission | Displays video admission control on the AP. |
| bandwidth | Displays video bandwidth on the AP. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to troubleshoot the access point AP01's transmit queue traffic on an 802.11a network:

```
(Cisco Controller) >debug ap show stats 802.11a AP01 tx-queue
```

The following example shows how to troubleshoot the access point AP02's multicast supported rates on an 802.11b/g network:

```
(Cisco Controller) >debug ap show stats 802.11b AP02 multicast
```

The following example shows how to troubleshoot the metrics of a client identified by its MAC address, associated with the access point AP01 on an 802.11a network:

```
(Cisco Controller) >debug ap show stats 802.11a AP01 client 00:40:96:a8:f7:98
```

The following example shows how to troubleshoot the metrics of all clients associated with the access point AP01 on an 802.11a network:

```
(Cisco Controller) >debug ap show stats 802.11a AP01 client all
```

debug ap show stats video

To configure the debugging of video messages and statistics of Cisco lightweight access points, use the **debug ap show stats video** command.

```
debug ap show stats video cisco_ap { multicast mgid mgid_value | admission | bandwidth }
```

| Syntax Description | | |
|--------------------|-----------------------|--|
| | <i>cisco_ap</i> | Cisco lightweight access point name. |
| | multicast mgid | Displays multicast database related information for the specified MGID of an access point. |
| | <i>mgid_value</i> | Layer 2 MGID database number from 1 to 4095. |
| | admission | Displays the video admission control. |
| | bandwidth | Displays the video bandwidth. |

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to configure the debugging of an access point AP01's multicast group that is identified by the group's Layer 2 MGID database number:

```
(Cisco Controller) >debug ap show stats video AP01 multicast mgid 50
```

This example shows how to configure the debugging of an access point AP01's video bandwidth:

```
(Cisco Controller) >debug ap show stats video AP01 bandwidth
```

debug capwap

To configure the debugging of Control and Provisioning of Wireless Access Points (CAPWAP) settings, use the **debug capwap** command.

debug capwap {**detail** | **dtls-keepalive** | **errors** | **events** | **hexdump** | **info** | **packet** | **payload** | **mfp**} {**enable** | **disable**}

Syntax Description

| | |
|-----------------------|---|
| detail | Configures the debugging for CAPWAP detail settings. |
| dtls-keepalive | Configures the debugging for CAPWAP DTLS data keepalive packets settings. |
| errors | Configures the debugging for CAPWAP error settings. |
| events | Configures the debugging for CAPWAP events settings. |
| hexdump | Configures the debugging for CAPWAP hexadecimal dump settings. |
| info | Configures the debugging for CAPWAP info settings. |
| packet | Configures the debugging for CAPWAP packet settings. |
| payload | Configures the debugging for CAPWAP payload settings. |
| mfp | Configures the debugging for CAPWAP mfp settings. |
| enable | Enables the debugging of the CAPWAP command. |
| disable | Disables the debugging of the CAPWAP command. |

Command Default

None

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

The following example shows how to enable the debugging of CAPWAP details:

```
(Cisco Controller) >debug capwap detail enable
```

debug lwapp console cli

To configure the debugging of the access point console CLI, use the **debug lwapp console cli** command from the access point console port.

debug lwapp console cli

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines This access point CLI command must be entered from the access point console port.

The following example shows how to configure the debugging of the access point console:

```
AP# debug lwapp console cli
LWAPP console CLI allow/disallow debugging is on
```

debug service ap-monitor

To debug the access point monitor service, use the **debug service ap-monitor** command.

debug service ap-monitor { **all** | **error** | **event** | **nmsp** | **packet** } { **enable** | **disable** }

| Syntax Description | | |
|--------------------|----------------|--|
| | all | Configures the debugging of all access point status messages. |
| | error | Configures the debugging of access point monitor error events. |
| | event | Configures the debugging of access point monitor events. |
| | nmsp | Configures the debugging of access point monitor Network Mobility Services Protocol (NMSP) events. |
| | packet | Configures the debugging of access point monitor packets. |
| | enable | Enables the debugging for access point monitor service. |
| | disable | Disables the debugging for access point monitor service. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to configure the debugging of access point monitor NMSP events:

```
(Cisco Controller) >debug service ap-monitor events
```

reset system at

To reset the system at a specified time, use the **reset system at** command.

```
reset system at YYYY-MM-DD HH:MM:SS image {no-swap | swap} reset-aps [save-config]
```

| Syntax Description | | |
|--------------------|--------------------|---|
| | YYYY-MM-DD | Specifies the date. |
| | HH:MM:SS | Specifies the time in a 24-hour format. |
| | image | Configures the image to be rebooted. |
| | swap | Changes the active boot image; boots the non-active image and sets the default flag on it on the next reboot. |
| | no-swap | Boots from the active image. |
| | reset-aps | Resets all access points during the system reset. |
| | save-config | (Optional) Saves the configuration before the system reset. |

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to reset the system at 2010-03-29 and 12:01:01 time:

```
(Cisco Controller) > reset system at 2010-03-29 12:01:01 image swap reset-aps save-config
```

Related Topics

- [reset system in](#)
- [reset system notify-time](#)

reset system in

To specify the amount of time delay before the devices reboot, use the **reset system in** command.

reset system in HH:MM:SS image {swap | no-swap} reset-aps save-config

| Syntax Description | | |
|--------------------|--------------------|---|
| | HH:MM:SS | Specifies a delay in duration. |
| | image | Configures the image to be rebooted. |
| | swap | Changes the active boot image; boots the non-active image and sets the default flag on it on the next reboot. |
| | reset-aps | Resets all access points during the system reset. |
| | save-config | Saves the configuration before the system reset. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to reset the system after a delay of 00:01:01:

```
(Cisco Controller) > reset system in 00:01:01 image swap reset-aps save-config
```

Related Topics

[reset system at](#)

[reset system notify-time](#)

reset system cancel

To cancel a scheduled reset, use the **reset system cancel** command.

reset system cancel

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to cancel a scheduled reset:

```
(Cisco Controller) > reset system cancel
```

Related Topics

- [reset system at](#)
- [reset system in](#)
- [reset system notify-time](#)

reset system notify-time

To configure the trap generation prior to scheduled resets, use the **reset system notify-time** command.

reset system notify-time *minutes*

| | | |
|---------------------------|---|--|
| Syntax Description | <i>minutes</i> | Number of minutes before each scheduled reset at which to generate a trap. |
| Command Default | The default time period to configure the trap generation prior to scheduled resets is 10 minutes. | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to configure the trap generation to 10 minutes before the scheduled resets:

```
(Cisco Controller) > reset system notify-time 55
```

show advanced max-1x-sessions

To display the maximum number of simultaneous 802.1X sessions allowed per access point, use the **show advanced max-1x-sessions** command.

show advanced max-1x-sessions

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|------------------------|------|
| Command Default | None |
|------------------------|------|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display the maximum 802.1X sessions per access point:

```
(Cisco Controller) >show advanced max-1x-sessions
Max 802.1x session per AP at a given time..... 0
```

show advanced probe

To display the number of probes sent to the Cisco WLC per access point per client and the probe interval in milliseconds, use the **show advanced probe** command.

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display the probe settings for the WLAN controller:

```
(Cisco Controller) >show advanced probe
Probe request filtering..... Enabled
Probes fwd to controller per client per radio.... 12
Probe request rate-limiting interval..... 100 msec
```

show advanced timers

To display the mobility anchor, authentication response, and rogue access point entry timers, use the **show advanced timers** command.

show advanced timers

Syntax Description

This command has no arguments or keywords.

Command Default

The defaults are shown in the “Examples” section.

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

The following example shows how to display the system timers setting:

```
(Cisco Controller) >show advanced timers
Authentication Response Timeout (seconds)..... 10
Rogue Entry Timeout (seconds)..... 1200
AP Heart Beat Timeout (seconds)..... 30
AP Discovery Timeout (seconds)..... 10
AP Local mode Fast Heartbeat (seconds)..... disable
AP flexconnect mode Fast Heartbeat (seconds)..... disable
AP Primary Discovery Timeout (seconds)..... 120
```

show ap auto-rf

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap auto-rf** command.

show ap auto-rf 802.11{a | b} *cisco_ap*

| | | |
|---------------------------|-----------------|--------------------------------------|
| Syntax Description | a | Specifies the 802.11a network. |
| | b | Specifies the 802.11b/g network. |
| | <i>cisco_ap</i> | Cisco lightweight access point name. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to display auto-RF information for an access point:

```
(Cisco Controller) > show ap auto-rf 802.11a AP1
Number Of Slots..... 2
AP Name..... AP03
MAC Address..... 00:0b:85:01:18:b7
Radio Type..... RADIO_TYPE_80211a
Noise Information
  Noise Profile..... PASSED
  Channel 36..... -88 dBm
  Channel 40..... -86 dBm
  Channel 44..... -87 dBm
  Channel 48..... -85 dBm
  Channel 52..... -84 dBm
  Channel 56..... -83 dBm
  Channel 60..... -84 dBm
  Channel 64..... -85 dBm
Interference Information
  Interference Profile..... PASSED
  Channel 36..... -66 dBm @ 1% busy
  Channel 40..... -128 dBm @ 0% busy
  Channel 44..... -128 dBm @ 0% busy
  Channel 48..... -128 dBm @ 0% busy
  Channel 52..... -128 dBm @ 0% busy
  Channel 56..... -73 dBm @ 1% busy
  Channel 60..... -55 dBm @ 1% busy
  Channel 64..... -69 dBm @ 1% busy
Rogue Histogram (20/40_ABOVE/40_BELOW)
  Channel 36..... 16/ 0/ 0
  Channel 40..... 28/ 0/ 0
  Channel 44..... 9/ 0/ 0
  Channel 48..... 9/ 0/ 0
```

```

Channel 52..... 3/ 0/ 0
Channel 56..... 4/ 0/ 0
Channel 60..... 7/ 1/ 0
Channel 64..... 2/ 0/ 0
Load Information
  Load Profile..... PASSED
  Receive Utilization..... 0%
  Transmit Utilization..... 0%
  Channel Utilization..... 1%
  Attached Clients..... 1 clients
Coverage Information
  Coverage Profile..... PASSED
  Failed Clients..... 0 clients
Client Signal Strengths
  RSSI -100 dBm..... 0 clients
  RSSI -92 dBm..... 0 clients
  RSSI -84 dBm..... 0 clients
  RSSI -76 dBm..... 0 clients
  RSSI -68 dBm..... 0 clients
  RSSI -60 dBm..... 0 clients
  RSSI -52 dBm..... 0 clients
Client Signal To Noise Ratios
  SNR 0 dBm..... 0 clients
  SNR 5 dBm..... 0 clients
  SNR 10 dBm..... 0 clients
  SNR 15 dBm..... 0 clients
  SNR 20 dBm..... 0 clients
  SNR 25 dBm..... 0 clients
  SNR 30 dBm..... 0 clients
  SNR 35 dBm..... 0 clients
  SNR 40 dBm..... 0 clients
  SNR 45 dBm..... 0 clients
Nearby RADs
  RAD 00:0b:85:01:05:08 slot 0..... -46 dBm on 10.1.30.170
  RAD 00:0b:85:01:12:65 slot 0..... -24 dBm on 10.1.30.170
Channel Assignment Information
  Current Channel Average Energy..... -86 dBm
  Previous Channel Average Energy..... -75 dBm
  Channel Change Count..... 109
  Last Channel Change Time..... Wed Sep 29 12:53e:34
2004
  Recommended Best Channel..... 44
RF Parameter Recommendations
  Power Level..... 1
  RTS/CTS Threshold..... 2347
  Fragmentation Threshold..... 2346
  Antenna Pattern..... 0

```

show ap cdp

To display the Cisco Discovery Protocol (CDP) information for an access point, use the **show ap cdp** command.

```
show ap cdp {all | ap-name cisco_ap | neighbors {all | ap-name cisco_ap | detail cisco_ap}}
```

| Syntax Description | | |
|--------------------|--|--|
| all | | Displays the CDP status on all access points. |
| ap-name | | Displays the CDP status for a specified access point. |
| <i>cisco_ap</i> | | Specified access point name. |
| neighbors | | Displays neighbors using CDP. |
| detail | | Displays details about a specific access point neighbor using CDP. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display the CDP status of all access points:

```
(Cisco Controller) >show ap cdp all
AP CDP State
AP Name          AP CDP State
-----
SB_RAP1          enable
SB_MAP1          enable
SB_MAP2          enable
SB_MAP3          enable
```

The following example shows how to display the CDP status of a specified access point:

```
(Cisco Controller) >show ap cdp ap-name SB_RAP1
AP CDP State
AP Name          AP CDP State
-----
AP CDP State.....Enabled
AP Interface-Based CDP state
 Ethernet 0.....Enabled
  Slot 0.....Enabled
  Slot 1.....Enabled
```

The following example shows how to display details about all neighbors using CDP:

```
(Cisco Controller) >show ap cdp neighbor all
AP Name      AP IP      Neighbor Name      Neighbor IP      Neighbor Port
-----
-----
```



```

SB_RAP1      192.168.102.154  sjc14-41a-sw1      192.168.102.2      GigabitEthernet1/0/13
SB_RAP1      192.168.102.154  SB_MAP1            192.168.102.137    Virtual-Dot11Radio0
SB_MAP1      192.168.102.137  SB_RAP1            192.168.102.154    Virtual-Dot11Radio0
SB_MAP1      192.168.102.137  SB_MAP2            192.168.102.138    Virtual-Dot11Radio0
SB_MAP2      192.168.102.138  SB_MAP1            192.168.102.137    Virtual-Dot11Radio1
SB_MAP2      192.168.102.138  SB_MAP3            192.168.102.139    Virtual-Dot11Radio0
SB_MAP3      192.168.102.139  SB_MAP2            192.168.102.138    Virtual-Dot11Radio1

```

The following example shows how to display details about a specific neighbor with a specified access point using CDP:

```

(Cisco Controller) >show ap cdp neighbors ap-name SB_MAP2
AP Name      AP IP      Neighbor Name  Neighbor IP  Neighbor Port
-----
SB_MAP2      192.168.102.138  SB_MAP1      192.168.102.137  Virtual-Dot11Radio1
SB_MAP2      192.168.102.138  SB_MAP3      192.168.102.139  Virtual-Dot11Radio0

```

The following example shows how to display details about neighbors using CDP:

```

(Cisco Controller) >show ap cdp neighbors detail SB_MAP2
AP Name:SB_MAP2
AP IP address:192.168.102.138
-----
Device ID: SB_MAP1
Entry address(es): 192.168.102.137
Platform: cisco AIR-LAP1522AG-A-K9 , Cap
Interface: Virtual-Dot11Radio0, Port ID (outgoing port): Virtual-Dot11Radio1
Holdtime : 180 sec
Version :
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Experimental Version 12.4(20081114:084420) [BLD-v124_18a_ja_throttle.20081114 208] Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Fri 14-Nov-08 23:08 by advertisement version: 2
-----
Device ID: SB_MAP3
Entry address(es): 192.168.102.139
Platform: cisco AIR-LAP1522AG-A-K9 , Capabilities: Trans-Bridge
Interface: Virtual-Dot11Radio1, Port ID (outgoing port): Virtual-Dot11Radio0
Holdtime : 180 sec
Version :
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Experimental Version 12.4(20081114:084420) [BLD-v124_18a_ja_throttle.20081114 208] Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Fri 14-Nov-08 23:08 by advertisement version: 2

```

show ap channel

To display the available channels for a specific mesh access point, use the **show ap channel** command.

show ap channel *ap_name*

| | | |
|---------------------------|----------------|--------------------------------|
| Syntax Description | <i>ap_name</i> | Name of the mesh access point. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to display the available channels for a particular access point:

```
(Cisco Controller) >show ap channel AP47
 802.11b/g Current Channel .....1
Allowed Channel List.....1,2,3,4,5,6,7,8,9,10,11
802.11a Current Channel .....161
Allowed Channel List.....36,40,44,48,52,56,60,64,100,
.....104,108,112,116,132,136,140,
.....149,153,157,161
```

show ap config

To display the detailed configuration for a lightweight access point, use the **show ap config** command.

```
show ap config 802.11{a | b} [summary] cisco_ap
```

| Syntax Description | 802.11a | Specifies the 802.11a or 802.11b/g network. |
|--------------------|----------|--|
| | 802.11b | Specifies the 802.11b/g network. |
| | summary | (Optional) Displays radio summary of all APs |
| | cisco_ap | Lightweight access point name. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to display the detailed configuration for an access point:

```
(Cisco Controller) >show ap config 802.11a AP02
Cisco AP Identifier..... 0
Cisco AP Name..... AP02
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-A 802.11a:-A
AP Regulatory Domain..... Unconfigured
Switch Port Number ..... 1
MAC Address..... 00:0b:85:18:b6:50
IP Address Configuration..... DHCP
IP Address..... 1.100.49.240
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 1.100.49.1
CAPWAP Path MTU..... 1485
Telnet State..... Disabled
Ssh State..... Disabled
Cisco AP Location..... default-location
Cisco AP Group Name..... default-group
Primary Cisco Switch..... Cisco_32:ab:63
Primary Cisco Switch IP Address..... Not Configured
Secondary Cisco Switch.....
Secondary Cisco Switch IP Address..... Not Configured
Tertiary Cisco Switch.....
Tertiary Cisco Switch IP Address..... Not Configured
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Sniffer
Public Safety ..... Global: Disabled, Local: Disabled
AP SubMode ..... Not Configured
Remote AP Debug ..... Disabled
Logging trap severity level ..... informational
Logging syslog facility ..... kern
S/W Version ..... 7.0.110.6
Boot Version ..... 12.4.18.0
```

show ap config

```

Mini IOS Version ..... 3.0.51.0
Stats Reporting Period ..... 180
Stats Re--More-- or (q)uit
LED State..... Enabled
PoE Pre-Standard Switch..... Enabled
PoE Power Injector MAC Addr..... Disabled
Power Type/Mode..... Power injector / Normal mode
Number Of Slots..... 2
AP Model..... AIR-LAP1142N-A-K9
AP Image..... C1140-K9W8-M
IOS Version..... 12.4(20100502:031212)
Reset Button..... Enabled
AP Serial Number..... FTX1305S180
AP Certificate Type..... Manufacture Installed
AP User Mode..... AUTOMATIC
AP User Name..... Not Configured
AP Dot1x User Mode..... Not Configured
AP Dot1x User Name..... Not Configured
Cisco AP system logging host..... 255.255.255.255
AP Up Time..... 47 days, 23 h 47 m 47 s
AP LWAPP Up Time..... 47 days, 23 h 10 m 37 s
Join Date and Time..... Tue May 4 16:05:00 2010
Join Taken Time..... 0 days, 00 h 01 m 37 s
Attributes for Slot 1
  Radio Type..... RADIO_TYPE_80211n-5
  Radio Subband..... RADIO_SUBBAND_ALL
  Administrative State ..... ADMIN_ENABLED
  Operation State ..... UP
  Radio Role ..... ACCESS
  CellId ..... 0
Station Configuration
  Configuration ..... AUTOMATIC
  Number Of WLANs ..... 2
  Medium Occupancy Limit ..... 100
  CFP Period ..... 4
  CFP MaxDuration ..... 60
  BSSID ..... 00:24:97:88:99:60
Operation Rate Set
  6000 Kilo Bits..... MANDATORY
  9000 Kilo Bits..... SUPPORTED
  12000 Kilo Bits..... MANDATORY
  18000 Kilo Bits..... SUPPORTED
  24000 Kilo Bits..... MANDATORY
  36000 Kilo Bits..... SUPPORTED
  48000 Kilo Bits..... SUPPORTED
  54000 Kilo Bits..... SUPPORTED
MCS Set
  MCS 0..... SUPPORTED
  MCS 1..... SUPPORTED
  MCS 2..... SUPPORTED
  MCS 3..... SUPPORTED
  MCS 4..... SUPPORTED
  MCS 5..... SUPPORTED
  MCS 6..... SUPPORTED
  MCS 7..... SUPPORTED
  MCS 8..... SUPPORTED
  MCS 9..... SUPPORTED
  MCS 10..... SUPPORTED
  MCS 11..... SUPPORTED
  MCS 12..... SUPPORTED
  MCS 13..... SUPPORTED
  MCS 14..... SUPPORTED
  MCS 15..... SUPPORTED
Beacon Period ..... 100

```

```

Fragmentation Threshold ..... 2346
Multi Domain Capability Implemented ..... TRUE
Multi Domain Capability Enabled ..... TRUE
Country String ..... US
Multi Domain Capability
  Configuration ..... AUTOMATIC
  First Chan Num ..... 36
  Number Of Channels ..... 21
MAC Operation Parameters
  Configuration ..... AUTOMATIC
  Fragmentation Threshold ..... 2346
  Packet Retry Limit ..... 64
Tx Power
  Num Of Supported Power Levels ..... 6
  Tx Power Level 1 ..... 14 dBm
  Tx Power Level 2 ..... 11 dBm
  Tx Power Level 3 ..... 8 dBm
  Tx Power Level 4 ..... 5 dBm
  Tx Power Level 5 ..... 2 dBm
  Tx Power Level 6 ..... -1 dBm
  Tx Power Configuration ..... AUTOMATIC
  Current Tx Power Level ..... 0
Phy OFDM parameters
  Configuration ..... AUTOMATIC
  Current Channel ..... 36
  Extension Channel ..... NONE
  Channel Width..... 20 Mhz
  Allowed Channel List..... 36,40,44,48,52,56,60,64,100,
    ..... 104,108,112,116,132,136,140,
    ..... 149,153,157,161,165
  TI Threshold ..... -50
  Legacy Tx Beamforming Configuration ..... AUTOMATIC
  Legacy Tx Beamforming ..... DISABLED
  Antenna Type..... INTERNAL_ANTENNA
  Internal Antenna Gain (in .5 dBi units).... 6
  Diversity..... DIVERSITY_ENABLED
802.11n Antennas
  Tx
    A..... ENABLED
    B..... ENABLED
  Rx
    A..... ENABLED
    B..... ENABLED
    C..... ENABLED
Performance Profile Parameters
  Configuration ..... AUTOMATIC
  Interference threshold..... 10 %
  Noise threshold..... -70 dBm
  RF utilization threshold..... 80 %
  Data-rate threshold..... 1000000 bps
  Client threshold..... 12 clients
  Coverage SNR threshold..... 16 dB
  Coverage exception level..... 25 %
  Client minimum exception level..... 3 clients
Rogue Containment Information
  Containment Count..... 0
CleanAir Management Information
  CleanAir Capable..... No
Radio Extended Configurations:
  Buffer size .....30
  Data-rate.....0
  Beacon strt .....90 ms
  Rx-Sensitivity SOP threshold ..... -80 dB

```

```
CCA threshold ..... -60 dB
```

The following example shows how to display the detailed configuration for another access point:

```
(Cisco Controller) >show ap config 802.11b AP02
Cisco AP Identifier..... 0
Cisco AP Name..... AP02
AP Regulatory Domain..... Unconfigured
Switch Port Number ..... 1
MAC Address..... 00:0b:85:18:b6:50
IP Address Configuration..... DHCP
IP Address..... 1.100.49.240
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 1.100.49.1
Cisco AP Location..... default-location
Cisco AP Group Name..... default-group
Primary Cisco Switch..... Cisco_32:ab:63
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Remote AP Debug ..... Disabled
S/W Version ..... 3.1.61.0
Boot Version ..... 1.2.59.6
Stats Reporting Period ..... 180
LED State..... Enabled
ILP Pre Standard Switch..... Disabled
ILP Power Injector..... Disabled
Number Of Slots..... 2
AP Model..... AS-1200
AP Serial Number..... 044110223A
AP Certificate Type..... Manufacture Installed
Attributes for Slot 1
  Radio Type..... RADIO_TYPE_80211g
  Administrative State ..... ADMIN_ENABLED
  Operation State ..... UP
  CellId ..... 0
  Station Configuration
    Configuration ..... AUTOMATIC
    Number Of WLANs ..... 1
    Medium Occupancy Limit ..... 100
    CFP Period ..... 4
    CFP MaxDuration ..... 60
    BSSID ..... 00:0b:85:18:b6:50
  Operation Rate Set
    1000 Kilo Bits..... MANDATORY
    2000 Kilo Bits..... MANDATORY
    5500 Kilo Bits..... MANDATORY
    11000 Kilo Bits..... MANDATORY
    6000 Kilo Bits..... SUPPORTED
    9000 Kilo Bits..... SUPPORTED
    12000 Kilo Bits..... SUPPORTED
    18000 Kilo Bits..... SUPPORTED
    24000 Kilo Bits..... SUPPORTED
    36000 Kilo Bits..... SUPPORTED
    48000 Kilo Bits..... SUPPORTED
    54000 Kilo Bits..... SUPPORTED
  Beacon Period ..... 100
  DTIM Period ..... 1
  Fragmentation Threshold ..... 2346
  Multi Domain Capability Implemented ..... TRUE
```

```

Multi Domain Capability Enabled ..... TRUE
Country String ..... US
Multi Domain Capability
Configuration ..... AUTOMATIC
First Chan Num ..... 1
Number Of Channels ..... 11
MAC Operation Parameters
Configuration ..... AUTOMATIC
RTS Threshold ..... 2347
Short Retry Limit ..... 7
Long Retry Limit ..... 4
Fragmentation Threshold ..... 2346
Maximum Tx MSDU Life Time ..... 512
Maximum Rx Life Time..... 512
Tx Power
Num Of Supported Power Levels..... 5
Tx Power Level 1 ..... 17 dBm
Tx Power Level 2..... 14 dBm
Tx Power Level 3..... 11 dBm
Tx Power Level 4..... 8 dBm
Tx Power Level 5..... 5 dBm
Tx Power Configuration..... CUSTOMIZED
Current Tx Power Level..... 5
Phy OFDM parameters
Configuration..... CUSTOMIZED
Current Channel..... 1
TI Threshold..... -50
Legacy Tx Beamforming Configuration ..... CUSTOMIZED
Legacy Tx Beamforming ..... ENABLED
Antenna Type..... INTERNAL_ANTENNA
Internal Antenna Gain (in5 dBm units)..... 11
Diversity..... DIVERSITY_ENABLED
Performance Profile Parameters
Configuration..... AUTOMATIC
Interference threshold..... 10%
Noise threshold..... -70 dBm
RF utilization threshold..... 80%
Data-rate threshold..... 1000000 bps
Client threshold..... 12 clients
Coverage SNR threshold..... 12 dB
Coverage exception level..... 25%
Client minimum exception level..... 3 clients
Rogue Containment Information
Containment Count..... 0

```

The following example shows how to display the general configuration of a Cisco access point:

```

(Cisco Controller) >show ap config general cisco-ap
Cisco AP Identifier..... 9
Cisco AP Name..... cisco-ap
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-A 802.11a:-A
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-A
Switch Port Number ..... 1
MAC Address..... 12:12:12:12:12:12
IP Address Configuration..... DHCP
IP Address..... 10.10.10.21
IP NetMask..... 255.255.255.0
CAPWAP Path MTU..... 1485
Domain.....
Name Server.....
Telnet State..... Disabled

```

show ap config

```

Ssh State..... Disabled
Cisco AP Location..... default location
Cisco AP Group Name..... default-group
Primary Cisco Switch Name..... 4404
Primary Cisco Switch IP Address..... 10.10.10.32
Secondary Cisco Switch Name.....
Secondary Cisco Switch IP Address..... Not Configured
Tertiary Cisco Switch Name..... 4404
Tertiary Cisco Switch IP Address..... 3.3.3.3
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Public Safety ..... Global: Disabled, Local: Disabled
AP subMode ..... WIPS
Remote AP Debug ..... Disabled
S/W Version ..... 5.1.0.0
Boot Version ..... 12.4.10.0
Mini IOS Version ..... 0.0.0.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Enabled
PoE Power Injector MAC Addr..... Disabled
Power Type/Mode..... PoE/Low Power (degraded mode)
Number Of Slots..... 2
AP Model..... AIR-LAP1252AG-A-K9
IOS Version..... 12.4(10:0)
Reset Button..... Enabled
AP Serial Number..... serial_number
AP Certificate Type..... Manufacture Installed
Management Frame Protection Validation..... Enabled (Global MFP Disabled)
AP User Mode..... CUSTOMIZED
AP username..... maria
AP Dot1x User Mode..... Not Configured
AP Dot1x username..... Not Configured
Cisco AP system logging host..... 255.255.255.255
AP Up Time..... 4 days, 06 h 17 m 22 s
AP LWAPP Up Time..... 4 days, 06 h 15 m 00 s
Join Date and Time..... Mon Mar 3 06:19:47 2008
Ethernet Port Duplex..... Auto
Ethernet Port Speed..... Auto
AP Link Latency..... Enabled
  Current Delay..... 0 ms
  Maximum Delay..... 240 ms
  Minimum Delay..... 0 ms
  Last updated (based on AP Up Time)..... 4 days, 06 h 17 m 20 s
Rogue Detection..... Enabled
AP TCP MSS Adjust..... Disabled
Mesh preferred parent..... 00:24:13:0f:92:00

```


show ap config general

To display the access point specific syslog server settings for all access points, use the **show ap config general** command.

show ap config general *ap-name*

| Syntax Description | <i>ap-name</i> | AP name |
|--------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

show ap config global

To display the global syslog server settings for all access points that join the controller, use the **show ap config global** command.

show ap config global

Syntax Description

This command has no arguments and keywords.

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

The following example shows how to display global syslog server settings:

```
(Cisco Controller) >show ap config global
AP global system logging host..... 255.255.255.255
```

show ap core-dump

To display the memory core dump information for a lightweight access point, use the **show ap core-dump** command.

show ap core-dump *cisco_ap*

| | | |
|---------------------------|-----------------|--------------------------------------|
| Syntax Description | <i>cisco_ap</i> | Cisco lightweight access point name. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to display memory core dump information:

```
(Cisco Controller) >show ap core-dump AP02  
Memory core dump is disabled.
```

show ap crash-file

To display the list of both crash and radio core dump files generated by lightweight access points, use the **show ap crash-file** command.

show ap crash-file

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display the crash file generated by the access point:

```
(Cisco Controller) >show ap crash-file
```

show ap data-plane

To display the data plane status for all access points or a specific access point, use the **show ap data-plane** command.

show ap data-plane {all | *cisco_ap*}

| | | |
|---------------------------|-----------------|--|
| Syntax Description | all | Specifies all Cisco lightweight access points. |
| | <i>cisco_ap</i> | Name of a Cisco lightweight access point. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to display the data plane status of all access points:

```
(Cisco Controller) >show ap data-plane all
Min Data      Data      Max Data      Last
AP Name      Round Trip      Round Trip      Round Trip      Update
-----
1130              0.000s              0.000s              0.002s      18:51:23
1240              0.000s              0.000s              0.000s      18:50:45
```

show ap dtls-cipher-suite

To display the DTLS show cipher suite information, use the **show ap dtls-cipher-suite** command.

show ap dtls-cipher-suite

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display DTLS cipher suite information:

```
(Cisco Controller) > show ap dtls-cipher-suite
DTLS Cipher Suite..... RSA-AES256-SHA
```

show ap ethernet tag

To display the VLAN tagging information of an Ethernet interface, use the **show ap ethernet tag** command.

```
show ap ethernet tag {summary | cisco_ap}
```

Syntax Description

| | |
|-----------------|---|
| summary | Displays the VLAN tagging information for all access points associated to the controller. |
| <i>cisco_ap</i> | Name of the Cisco lightweight access point. Displays the VLAN tagging information for a specific access point associated to the controller. |

Command Default

None

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

Usage Guidelines

If the access point is unable to route traffic or reach the controller using the specified trunk VLAN, it falls back to the untagged configuration. If the access point joins the controller using this fallback configuration, the controller sends a trap to a trap server such as the WCS, which indicates the failure of the trunk VLAN. In this scenario, the "Failover to untagged" message appears in show command output.

The following example shows how to display the VLAN tagging information for all access points associated to the controller:

```
(Cisco Controller) >show ap ethernet tag summary

AP Name           Vlan Tag Configuration
-----
AP2               7 (Failover to untagged)
charan.AP1140.II disabled
```

show ap eventlog

To display the contents of the event log file for an access point that is joined to the controller, use the **show ap eventlog** command.

show ap eventlog *ap_name*

| | | |
|---------------------------|----------------|---|
| Syntax Description | <i>ap_name</i> | Event log for the specified access point. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to display the event log of an access point:

```
(Cisco Controller) >show ap eventlog ciscoAP
AP event log download has been initiated
Waiting for download to complete
AP event log download completed.
===== AP Event log Contents =====
*Feb 13 11:54:17.146: %CAPWAP-3-CLIENTEVENTLOG: AP event log has been cleared from the
contoller 'admin'
*Feb 13 11:54:32.874: *** Access point reloading. Reason: Reload Command ***
*Mar 1 00:00:39.134: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
*Mar 1 00:00:39.174: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Mar 1 00:00:39.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar 1 00:00:49.947: %CAPWAP-3-CLIENTEVENTLOG: Did not get vendor specific options from
DHCP.
...
```


show ap image

To display the detailed information about the predownloaded image for specified access points, use the **show ap image** command.

```
show ap image {cisco_ap | all}
```

Syntax Description

| | |
|-----------------|---------------------------------------|
| <i>cisco_ap</i> | Name of the lightweight access point. |
| all | Specifies all access points. |



Note

If you have an AP that has the name *all*, it conflicts with the keyword **all** that specifies all access points. In this scenario, the keyword **all** takes precedence over the AP that is named *all*.

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

show ap inventory

To display inventory information for an access point, use the **show ap inventory** command.

```
show ap inventory {ap-name | all}
```

| | | |
|---------------------------|----------------|---------------------------------|
| Syntax Description | <i>ap-name</i> | Inventory for the specified AP. |
| | all | Inventory for all the APs. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

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

```
(Cisco Controller) >show ap inventory test101
NAME: "test101" , DESCR: "Cisco Wireless Access Point"
PID: AIR-LAP1131AG-A-K9 , VID: V01, SN: FTX1123T2XX
```

show ap join stats detailed

To display all join-related statistics collected for a specific access point, use the **show ap join stats detailed** command.

show ap join stats detailed *ap_mac*

| | | |
|---------------------------|----------------|---|
| Syntax Description | <i>ap_mac</i> | Access point Ethernet MAC address or the MAC address of the 802.11 radio interface. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to display join information for a specific access point trying to join the controller:

```
(Cisco Controller) >show ap join stats detailed 00:0b:85:02:0d:20
Discovery phase statistics
- Discovery requests received..... 2
- Successful discovery responses sent..... 2
- Unsuccessful discovery request processing..... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt..... Aug 21 12:50:23:335
- Time at last unsuccessful discovery attempt..... Not applicable
Join phase statistics
- Join requests received..... 1
- Successful join responses sent..... 1
- Unsuccessful join request processing..... 1
- Reason for last unsuccessful join attempt.....RADIUS authorization is pending for
the AP
- Time at last successful join attempt..... Aug 21 12:50:34:481
- Time at last unsuccessful join attempt..... Aug 21 12:50:34:374
Configuration phase statistics
- Configuration requests received..... 1
- Successful configuration responses sent..... 1
- Unsuccessful configuration request processing..... 0
- Reason for last unsuccessful configuration attempt... Not applicable
- Time at last successful configuration attempt..... Aug 21 12:50:34:374
- Time at last unsuccessful configuration attempt..... Not applicable
Last AP message decryption failure details
- Reason for last message decryption failure..... Not applicable
Last AP disconnect details
- Reason for last AP connection failure..... Not applicable
Last join error summary
- Type of error that occurred last..... Lwapp join request rejected
- Reason for error that occurred last..... RADIUS authorization is pending for
the AP
- Time at which the last join error occurred..... Aug 21 12:50:34:374
```

show ap join stats summary

To display the last join error detail for a specific access point, use the **show ap join stats summary** command.

show ap join stats summary *ap_mac*

| | | |
|---------------------------|---|---|
| Syntax Description | <i>ap_mac</i> | Access point Ethernet MAC address or the MAC address of the 802.11 radio interface. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |
| Usage Guidelines | To obtain the MAC address of the 802.11 radio interface, enter the show interface command on the access point. | |

The following example shows how to display specific join information for an access point:

```
(Cisco Controller) >show ap join stats summary 00:0b:85:02:0d:20
Is the AP currently connected to controller..... No
Time at which the AP joined this controller last time..... Aug 21 12:50:36:061
Type of error that occurred last..... Lwapp join request
rejected
Reason for error that occurred last..... RADIUS authorization
is pending for the AP
Time at which the last join error occurred..... Aug 21 12:50:34:374
```

show ap join stats summary all

To display the MAC addresses of all the access points that are joined to the controller or that have tried to join, use the **show ap join stats summary all** command.

show ap join stats summary all

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display a summary of join information for all access points:

```
(Cisco Controller) >show ap join stats summary all
Number of APs..... 4
Base Mac          AP EthernetMac    AP Name    IP Address    Status
00:0b:85:57:bc:c0 00:0b:85:57:bc:c0 AP1130     10.10.163.217  Joined
00:1c:0f:81:db:80 00:1c:63:23:ac:a0 AP1140     10.10.163.216  Not joined
00:1c:0f:81:fc:20 00:1b:d5:9f:7d:b2 AP1        10.10.163.215  Joined
00:21:1b:ea:36:60 00:0c:d4:8a:6b:c1 AP2        10.10.163.214  Not joined
```

show ap led-state

To view the LED state of all access points or a specific access point, use the **show ap led-state** command.

```
show ap led-state {all | cisco_ap}
```

| Syntax Description | all | Shows the LED state for all access points. |
|--------------------|------------------------------|--|
| | <i>cisco_ap</i> | Name of the access point whose LED state is to be shown. |
| Command Default | The AP LED state is enabled. | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to get the LED state of all access points:

```
(Cisco Controller) >show ap led-state all
Global LED State: Enabled (default)
```

show ap led-flash

To display the LED flash status of an access point, use the **show ap led-flash** command.

show ap led-flash *cisco_ap*

| | |
|---------------------------|---|
| Syntax Description | <i>cisco_ap</i> Enter the name of the Cisco AP. |
|---------------------------|---|

| | |
|------------------------|------|
| Command Default | None |
|------------------------|------|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display the LED flash status of an access point:

```
(Cisco Controller) >show ap led-flash
```

show ap max-count summary

To display the maximum number of access points supported by the Cisco WLC, use the **show ap max-count summary** command.

show ap max-count summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following is a sample output of the **show ap max-count summary** command:

```
(Cisco Controller) >show ap max-count
The max number of AP's supported..... 500
```

Related Topics

[config ap max-count](#)

show ap monitor-mode summary

To display the current channel-optimized monitor mode settings, use the **show ap monitor-mode summary** command.

show ap monitor-mode summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display current channel-optimized monitor mode settings:

```
(Cisco Controller) >show ap monitor-mode summary
AP Name           Ethernet MAC      Status      Scanning Channel List
-----
AP_004            xx:xx:xx:xx:xx:xx Tracking        1, 6, 11, 4
```

show ap module summary

To view detailed information about the external module, for a specific Cisco AP or for all Cisco APs, use the **show ap module summary** command.

show ap module summary {*ap-name* | **all**}

| Syntax Description | |
|--------------------|---|
| | <i>ap-name</i> Cisco AP name that has the external module |
| | all All Cisco APs that have the external module |

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

show ap packet-dump status

To display access point Packet Capture configurations, use the **show ap packet-dump status** command.

show ap packet-dump status

Syntax Description

This command has no arguments or keywords.

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

Usage Guidelines

Packet Capture does not work during intercontroller roaming.

The controller does not capture packets created in the radio firmware and sent out of the access point, such as the beacon or probe response. Only packets that flow through the Radio driver in the Tx path are captured.

The following example shows how to display the access point Packet Capture configurations:

```
(Cisco Controller) >show ap packet-dump status
Packet Capture Status..... Stopped
FTP Server IP Address..... 0.0.0.0
FTP Server Path.....
FTP Server Username.....
FTP Server Password..... *****
Buffer Size for Capture..... 2048 KB
Packet Capture Time..... 45 Minutes
Packet Truncate Length..... Unspecified
Packet Capture Classifier..... None
```

show ap prefer-mode stats

To view prefer-mode global and per AP group statistics, use the **show ap prefer-mode stats** command.

show ap prefer-mode stats

| | |
|---------------------------|--|
| Syntax Description | stats Displays prefer-mode global and per AP group statistics |
|---------------------------|--|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 8.3 | This command was introduced. |

show ap retransmit

To display access point control packet retransmission parameters, use the **show ap retransmit** command.

```
show ap retransmit {all | cisco_ap}
```

| | | |
|---------------------------|-----------------|------------------------------|
| Syntax Description | all | Specifies all access points. |
| | <i>cisco_ap</i> | Name of the access point. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to display the control packet retransmission parameters of all access points on a network:

```
(Cisco Controller) >show ap retransmit all
Global control packet retransmit interval: 3 (default)
Global control packet retransmit count: 5 (default)
AP Name                Retransmit Interval  Retransmit count
-----
AP_004                 3 (default)         5 (WLC default),5 (AP default)
```

show ap stats

To display the statistics for a Cisco lightweight access point, use the **show ap stats** command.

show ap stats {802.11{a | b} | wlan | ethernet summary} *cisco_ap* [**tsm** {*client_mac* | all}]

| Syntax Description | | |
|------------------------|----------------|---|
| 802.11a | | Specifies the 802.11a network |
| 802.11b | | Specifies the 802.11b/g network. |
| wlan | | Specifies WLAN statistics. |
| ethernet | | Specifies AP ethernet interface statistics. |
| summary | | Displays ethernet interface summary of all the connected Cisco access points. |
| <i>cisco_ap</i> | | Name of the lightweight access point. |
| tsm | | (Optional) Specifies the traffic stream metrics. |
| <i>client_mac</i> | | (Optional) MAC address of the client. |
| all | | (Optional) Specifies all access points. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to display statistics of an access point for the 802.11b network:

```
(Cisco Controller) >show ap stats 802.11a Ibiza

Number Of Slots..... 2
AP Name..... Ibiza
MAC Address..... 44:2b:03:9a:8a:73
Radio Type..... RADIO_TYPE_80211a
Stats Information
  Number of Users..... 0
  TxFragmentCount..... 84628
  MulticastTxFrameCnt..... 84628
  FailedCount..... 0
  RetryCount..... 0
  MultipleRetryCount..... 0
  FrameDuplicateCount..... 0
  RtsSuccessCount..... 1
  RtsFailureCount..... 0
  AckFailureCount..... 0
  RxIncompleteFragment..... 0
  MulticastRxFrameCnt..... 0
  FcsErrorCount..... 20348857
  TxFrameCount..... 84628
```

```

WepUndecryptableCount..... 19907
TxFramesDropped..... 0
OEAP WMM Stats :
  Best Effort:
    Tx Frame Count..... 0
    Tx Failed Frame Count..... 0
    Tx Expired Count..... 0
    Tx Overflow Count..... 0
    Tx Queue Count..... 0
    Tx Queue Max Count..... 0
    Rx Frame Count..... 0
    Rx Failed Frame Count..... 0
  Background:
    Tx Frame Count..... 0
    Tx Failed Frame Count..... 0
    Tx Expired Count..... 0
    Tx Overflow Count..... 0
    Tx Queue Count..... 0
    Tx Queue Max Count..... 0
    Rx Frame Count..... 0
    Rx Failed Frame Count..... 0
  Video:
    Tx Frame Count..... 0
    Tx Failed Frame Count..... 0
    Tx Expired Count..... 0
    Tx Overflow Count..... 0
    Tx Queue Count..... 0
    Tx Queue Max Count..... 0
    Rx Frame Count..... 0
    Rx Failed Frame Count..... 0
  Voice:
    Tx Frame Count..... 0
    Tx Failed Frame Count..... 0
    Tx Expired Count..... 0
    Tx Overflow Count..... 0
    Tx Queue Count..... 0
    Tx Queue Max Count..... 0
    Rx Frame Count..... 0
    Rx Failed Frame Count..... 0

Rate Limiting Stats:
  Wlan 1:
    Number of Data Packets Received..... 592
    Number of Data Rx Packets Dropped..... 160
    Number of Data Bytes Received..... 160783
    Number of Data Rx Bytes Dropped..... 0
    Number of Realtime Packets Received..... 592
    Number of Realtime Rx Packets Dropped..... 0
    Number of Realtime Bytes Received..... 160783
    Number of Realtime Rx Bytes Dropped..... 0
    Number of Data Packets Sent..... 131
    Number of Data Tx Packets Dropped..... 0
    Number of Data Bytes Sent..... 23436
    Number of Data Tx Bytes Dropped..... 0
    Number of Realtime Packets Sent..... 131
    Number of Realtime Tx Packets Dropped..... 0
    Number of Realtime Bytes Sent..... 23436
    Number of Realtime Tx Bytes Dropped..... 0
  Call Admission Control (CAC) Stats
    Voice Bandwidth in use(% of config bw)..... 0
    Voice Roam Bandwidth in use(% of config bw).... 0
    Total channel MT free..... 0
    Total voice MT free..... 0
    Na Direct..... 0

```

show ap stats

```

    Na Roam..... 0
    Video Bandwidth in use(% of config bw)..... 0
    Video Roam Bandwidth in use(% of config bw)... 0
    Total BW in use for Voice(%)..... 0
    Total BW in use for SIP Preferred call(%)..... 0
WMM TSPEC CAC Call Stats
    Total num of voice calls in progress..... 0
    Num of roaming voice calls in progress..... 0
    Total Num of voice calls since AP joined..... 0
    Total Num of roaming calls since AP joined.... 0
    Total Num of exp bw requests received..... 0
    Total Num of exp bw requests admitted..... 0
    Num of voice calls rejected since AP joined... 0
    Num of roam calls rejected since AP joined.... 0
    Num of calls rejected due to insufficient bw... 0
    Num of calls rejected due to invalid params... 0
    Num of calls rejected due to PHY rate..... 0
    Num of calls rejected due to QoS policy..... 0
SIP CAC Call Stats
    Total Num of calls in progress..... 0
    Num of roaming calls in progress..... 0
    Total Num of calls since AP joined..... 0
    Total Num of roaming calls since AP joined.... 0
    Total Num of Preferred calls received..... 0
    Total Num of Preferred calls accepted..... 0
    Total Num of ongoing Preferred calls..... 0
    Total Num of calls rejected(Insuff BW)..... 0
    Total Num of roam calls rejected(Insuff BW)... 0
WMM Video TSPEC CAC Call Stats
    Total num of video calls in progress..... 0
    Num of roaming video calls in progress..... 0
    Total Num of video calls since AP joined..... 0
    Total Num of video roaming calls since AP j... 0
    Num of video calls rejected since AP joined... 0
    Num of video roam calls rejected since AP j... 0
    Num of video calls rejected due to insuffic... 0
    Num of video calls rejected due to invalid ... 0
    Num of video calls rejected due to PHY rate... 0
    Num of video calls rejected due to QoS poli... 0
SIP Video CAC Call Stats
    Total Num of video calls in progress..... 0
    Num of video roaming calls in progress..... 0
    Total Num of video calls since AP joined..... 0
    Total Num of video roaming calls since AP j... 0
    Total Num of video calls rejected(Insuff BW... 0
    Total Num of video roam calls rejected(Insu... 0
Band Select Stats
    Num of dual band client ..... 0
    Num of dual band client added..... 0
    Num of dual band client expired ..... 0
    Num of dual band client replaced..... 0
    Num of dual band client detected ..... 0
    Num of suppressed client ..... 0
    Num of suppressed client expired..... 0
    Num of suppressed client replaced..... 0

```


show ap summary

To display a summary of all lightweight access points attached to the controller, use the **show ap summary** command.

show ap summary [*cisco_ap*]

| | | |
|---------------------------|-----------------|--|
| Syntax Description | <i>cisco_ap</i> | (Optional) Type sequence of characters that make up the name of a specific AP or a group of APs, or enter a wild character search pattern. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

Usage Guidelines A list that contains each lightweight access point name, number of slots, manufacturer, MAC address, location, and the controller port number appears. When you specify

The following example shows how to display a summary of all connected access points:

```
(Cisco Controller) >show ap summary
Number of APs..... 2
Global AP username..... user
Global AP Dot1x username..... Not Configured
Number of APs..... 2
Global AP username..... user
Global AP Dot1x username..... Not Configured

AP Name          Slots  AP Model          Ethernet MAC      Location
Country  IP Address          Clients
-----
AP1140          2      AIR-LAP1142N-A-K9  f0:f7:55:75:f3:29  default
location        US    192.168.0.0        0
Access Points using IPv6 transport:
AP Name  Slots  AP Model          Ethernet MAC      Location          Country  IPv6
Address          Clients
-----
AP1040    2      AIR-LAP1042N-A-K9  00:40:96:b9:4b:89  default location  US
2001:DB8:0:1::1          0
```

show ap tcp-mss-adjust

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point, use the **show ap tcp-mss-adjust** command.

```
show ap tcp-mss-adjust {cisco_ap | all}
```

| Syntax Description | | |
|--------------------|-----------------|--|
| | <i>cisco_ap</i> | Specified lightweight access point name. |
| | all | Specifies all access points. |



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

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display Transmission Control Protocol (TCP) maximum segment size (MSS) information of all access points:

```
(Cisco Controller) >show ap tcp-mss-adjust all
AP Name          TCP State MSS Size
-----
AP-1140          enabled   536
AP-1240          disabled  -
AP-1130          disabled  -
```

show ap wlan

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point, use the **show ap wlan** command.

```
show ap wlan 802.11 { a | b } cisco_ap
```

| | | |
|---------------------------|----------------|----------------------------------|
| Syntax Description | 802.11a | Specifies the 802.11a network. |
| | 802.11b | Specifies the 802.11b/g network. |
| | <i>ap_name</i> | Lightweight access point name. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

The following example shows how to display BSSIDs of an access point for the 802.11b network:

```
(Cisco Controller) >show ap wlan 802.11b AP01
Site Name..... MY_AP_GROUP1
Site Description..... MY_AP_GROUP1
WLAN ID      Interface      BSSID
-----
1            management    00:1c:0f:81:fc:20
2            dynamic      00:1c:0f:81:fc:21
```

show auth-list

To display the access point authorization list, use the **show auth-list** command.

show auth-list

Syntax Description

This command has no arguments or keywords.

Command History

| Release | Modification |
|---------|------------------------------|
| 8.3 | This command was introduced. |

The following example shows how to display the access point authorization list:

```
(Cisco Controller) >show auth-list
Authorize APs against AAA..... disabled
Allow APs with Self-signed Certificate (SSC)... disabled
Mac Addr          Cert Type      Key Hash
-----
xx:xx:xx:xx:xx:xx  MIC
```

show client ap

To display the clients on a Cisco lightweight access point, use the **show client ap** command.

```
show client ap 802.11{a | b} cisco_ap
```

| | | |
|---------------------------|---|--------------------------------------|
| Syntax Description | 802.11a | Specifies the 802.11a network. |
| | 802.11b | Specifies the 802.11b/g network. |
| | <i>cisco_ap</i> | Cisco lightweight access point name. |
| Command Default | None | |
| Usage Guidelines | The show client ap command may list the status of automatically disabled clients. Use the show exclusionlist command to view clients on the exclusion list (blacklisted). | |
| Command History | Release | Modification |
| | 8.3 | This command was introduced. |

This example shows how to display client information on an access point:

```
(Cisco Controller) >show client ap 802.11b AP1
MAC Address      AP Id  Status      WLAN Id  Authenticated
-----
xx:xx:xx:xx:xx:xx    1  Associated    1        No
```

show boot

To display the primary and backup software build numbers with an indication of which is active, use the **show boot** command.

show boot

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines Each Cisco wireless LAN controller retains one primary and one backup operating system software load in nonvolatile RAM to allow controllers to boot off the primary load (default) or revert to the backup load when desired.

The following is a sample output of the **show boot** command:

```
(Cisco Controller) > show boot
Primary Boot Image..... 3.2.13.0 (active)
Backup Boot Image..... 3.2.15.0
```

Related Commands **config boot**

show country

To display the configured country and the radio types that are supported, use the **show country** command.

show country

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|------------------------|------|
| Command Default | None |
|------------------------|------|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display the configured countries and supported radio types:

```
(Cisco Controller) >show country
Configured Country..... United States
Configured Country Codes
US - United States..... 802.11a / 802.11b / 802.11g
```

show country channels

To display the radio channels supported in the configured country, use the **show country channels** command.

show country channels

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display the auto-RF channels for the configured countries:

```
(Cisco Controller) >show country channels
Configured Country..... United States
KEY: * = Channel is legal in this country and may be configured manually.
Configured Country..... United States
KEY: * = Channel is legal in this country and may be configured manually.
A = Channel is the Auto-RF default in this country.
. = Channel is not legal in this country.
C = Channel has been configured for use by Auto-RF.
x = Channel is available to be configured for use by Auto-RF.
-----:+++++-----
802.11BG :
Channels :          1 1 1 1 1
          : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----:+++++-----
          US : A * * * * A * * * * A . . .
-----:+++++-----
          802.11A : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
          : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----:+++++-----
          US : . A . A . A . A A A A * * * * * . . . * * * A A A A *
-----:+++++-----
```


show country supported

To display a list of the supported country options, use the **show country supported** command.

show country supported

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display a list of all the supported countries:

```
(Cisco Controller) >show country supported
Configured Country..... United States
Supported Country Codes
AR - Argentina..... 802.11a / 802.11b / 802.11g
AT - Austria..... 802.11a / 802.11b / 802.11g
AU - Australia..... 802.11a / 802.11b / 802.11g
BR - Brazil..... 802.11a / 802.11b / 802.11g
BE - Belgium..... 802.11a / 802.11b / 802.11g
BG - Bulgaria..... 802.11a / 802.11b / 802.11g
CA - Canada..... 802.11a / 802.11b / 802.11g
CH - Switzerland..... 802.11a / 802.11b / 802.11g
CL - Chile..... 802.11b / 802.11g
CN - China..... 802.11a / 802.11b / 802.11g
CO - Colombia..... 802.11b / 802.11g
CY - Cyprus..... 802.11a / 802.11b / 802.11g
CZ - Czech Republic..... 802.11a / 802.11b
DE - Germany..... 802.11a / 802.11b / 802.11g
DK - Denmark..... 802.11a / 802.11b / 802.11g
EE - Estonia..... 802.11a / 802.11b / 802.11g
ES - Spain..... 802.11a / 802.11b / 802.11g
FI - Finland..... 802.11a / 802.11b / 802.11g
FR - France..... 802.11a / 802.11b / 802.11g
GB - United Kingdom..... 802.11a / 802.11b / 802.11g
GI - Gibraltar..... 802.11a / 802.11b / 802.11g
GR - Greece..... 802.11a / 802.11b / 802.11g
HK - Hong Kong..... 802.11a / 802.11b / 802.11g
HU - Hungary..... 802.11a / 802.11b / 802.11g
ID - Indonesia..... 802.11b / 802.11g
IE - Ireland..... 802.11a / 802.11b / 802.11g
IN - India..... 802.11a / 802.11b / 802.11g
IL - Israel..... 802.11a / 802.11b / 802.11g
ILO - Israel (outdoor)..... 802.11b / 802.11g
IS - Iceland..... 802.11a / 802.11b / 802.11g
IT - Italy..... 802.11a / 802.11b / 802.11g
JP - Japan (J)..... 802.11a / 802.11b / 802.11g
J2 - Japan 2 (P)..... 802.11a / 802.11b / 802.11g
J3 - Japan 3 (U)..... 802.11a / 802.11b / 802.11g
KR - Korea Republic (C)..... 802.11a / 802.11b / 802.11g
KE - Korea Extended (K)..... 802.11a / 802.11b / 802.11g
LI - Liechtenstein..... 802.11a / 802.11b / 802.11g
LT - Lithuania..... 802.11a / 802.11b / 802.11g
LU - Luxembourg..... 802.11a / 802.11b / 802.11g
```

show country supported

```
LV - Latvia..... 802.11a / 802.11b / 802.11g
MC - Monaco..... 802.11a / 802.11b / 802.11g
MT - Malta..... 802.11a / 802.11b / 802.11g
MX - Mexico..... 802.11a / 802.11b / 802.11g
MY - Malaysia..... 802.11a / 802.11b / 802.11g
NL - Netherlands..... 802.11a / 802.11b / 802.11g
NZ - New Zealand..... 802.11a / 802.11b / 802.11g
NO - Norway..... 802.11a / 802.11b / 802.11g
PA - Panama..... 802.11b / 802.11g
PE - Peru..... 802.11b / 802.11g
PH - Philippines..... 802.11a / 802.11b / 802.11g
PL - Poland..... 802.11a / 802.11b / 802.11g
PT - Portugal..... 802.11a / 802.11b / 802.11g
RU - Russian Federation..... 802.11a / 802.11b / 802.11g
RO - Romania..... 802.11a / 802.11b / 802.11g
SA - Saudi Arabia..... 802.11a / 802.11b / 802.11g
SE - Sweden..... 802.11a / 802.11b / 802.11g
SG - Singapore..... 802.11a / 802.11b / 802.11g
SI - Slovenia..... 802.11a / 802.11b / 802.11g
SK - Slovak Republic..... 802.11a / 802.11b / 802.11g
TH - Thailand..... 802.11b / 802.11g
TR - Turkey..... 802.11b / 802.11g
TW - Taiwan..... 802.11a / 802.11b / 802.11g
UA - Ukraine..... 802.11a / 802.11b / 802.11g
US - United States..... 802.11a / 802.11b / 802.11g
USL - United States (Legacy)..... 802.11a / 802.11b / 802.11g
USX - United States (US + chan165)..... 802.11a / 802.11b / 802.11g
VE - Venezuela..... 802.11b / 802.11g
ZA - South Africa..... 802.11a / 802.11b / 802.11g
```

show dtls connections

To display the Datagram Transport Layer Security (DTLS) server status, use the **show dtls connections** command.

show dtls connections

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

The following is a sample output of the **show dtls connections** command.

Device > **show dtls connections**

| AP Name | Local Port | Peer IP | Peer Port | Ciphersuite |
|---------|-------------|---------------|-----------|------------------------------|
| 1130 | Capwap_Ctrl | 1.100.163.210 | 23678 | TLS_RSA_WITH_AES_128_CBC_SHA |
| 1130 | Capwap_Data | 1.100.163.210 | 23678 | TLS_RSA_WITH_AES_128_CBC_SHA |
| 1240 | Capwap_Ctrl | 1.100.163.209 | 59674 | TLS_RSA_WITH_AES_128_CBC_SHA |

show known ap

To display known Cisco lightweight access point information, use the **show known ap** command.

show known ap {**summary** | **detailed** *MAC*}

| Syntax Description | summary | Displays a list of all known access points. | | |
|--------------------|-----------------|--|--|--|
| | detailed | Provides detailed information for all known access points. | | |
| | <i>MAC</i> | MAC address of the known AP. | | |
| Command Default | None | | | |
| Command History | Release | Modification | | |
| | 8.3 | This command was introduced. | | |

The following example shows how to display a summary of all known access points:

```
(Cisco Controller) >show known ap summary
MAC Address      State      # APs  # Clients  Last Heard
-----
```

show msglog

To display the message logs written to the Cisco WLC database, use the **show msglog** command.

show msglog

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

Usage Guidelines If there are more than 15 entries, you are prompted to display the messages shown in the example.

The following example shows how to display message logs:

```
(Cisco Controller) >show msglog
Message Log Severity Level..... ERROR
Thu Aug 4 14:30:08 2005 [ERROR] spam_lrad.c 1540: AP 00:0b:85:18:b6:50 associated. Last
AP failure was due to Link Failure
Thu Aug 4 14:30:08 2005 [ERROR] spam_lrad.c 13840: Updating IP info for AP 00:
0b:85:18:b6:50 -- static 0, 1.100.49.240/255.255.255.0, gw 1.100.49.1
Thu Aug 4 14:29:32 2005 [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Thu Aug 4 14:29:32 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11a switch group
reset
Thu Aug 4 14:29:32 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Thu Aug 4 14:29:22 2005 [ERROR] sim.c 2841: Unable to get link state for primary port 0
of interface ap-manager
Thu Aug 4 14:29:22 2005 [ERROR] dtl_l2_dot1q.c 767: Unable to get USP
Thu Aug 4 14:29:22 2005 Previous message occurred 2 times
Thu Aug 4 14:29:14 2005 [CRITICAL] osapi_sem.c 794: Error! osapiMutexTake called with
NULL pointer: osapi_bsntime.c:927
Thu Aug 4 14:29:14 2005 [CRITICAL] osapi_sem.c 794: Error! osapiMutexTake called with
NULL pointer: osapi_bsntime.c:919
Thu Aug 4 14:29:14 2005 [CRITICAL] hwutils.c 1861: Security Module not found
Thu Aug 4 14:29:13 2005 [CRITICAL] bootos.c 791: Starting code...
```

show network summary

To display the network configuration of the Cisco wireless LAN controller, use the **show network summary** command.

show network summary

Syntax Description This command has no arguments or keywords.

Command Default None.

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.3 | This command was introduced. |

This example shows how to display a summary configuration:

```
(Cisco Controller) >show network summary
RF-Network Name..... RF
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Web Mode Cipher-Option High..... Disable
Secure Web Mode Cipher-Option SSLv2..... Disable
Secure Web Mode RC4 Cipher Preference..... Disable
OCSP..... Disabled
OCSP responder URL.....
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable   Mode: Ucast
Ethernet Broadcast Mode..... Disable
Ethernet Multicast Forwarding..... Disable
Ethernet Broadcast Forwarding..... Disable
AP Multicast/Broadcast Mode..... Unicast
IGMP snooping..... Disabled
IGMP timeout..... 60 seconds
IGMP Query Interval..... 20 seconds
MLD snooping..... Disabled
MLD timeout..... 60 seconds
MLD query interval..... 20 seconds
User Idle Timeout..... 300 seconds
AP Join Priority..... Disable
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Disable
Mgmt Via Dynamic Interface..... Disable
Bridge MAC filter Config..... Enable
Bridge Security Mode..... EAP
Over The Air Provisioning of AP's..... Enable
Apple Talk ..... Disable
Mesh Full Sector DFS..... Enable
AP Fallback ..... Disable
Web Auth CMCC Support ..... Disabled
Web Auth Redirect Ports ..... 80
Web Auth Proxy Redirect ..... Disable
Web Auth Captive-Bypass ..... Disable
Web Auth Secure Web ..... Enable
```

```
Fast SSID Change ..... Disabled
AP Discovery - NAT IP Only ..... Enabled
IP/MAC Addr Binding Check ..... Enabled
CCX-lite status ..... Disable
oep-600 dual-rlan-ports ..... Disable
oep-600 local-network ..... Enable
mDNS snooping..... Disabled
mDNS Query Interval..... 15 minutes
Web Color Theme..... Red
Web Color Theme..... Default
CAPWAP Prefer Mode..... IPv4
```

show watchlist

To display the client watchlist, use the **show watchlist** command.

show watchlist

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 8.3 | This command was introduced. |

The following example shows how to display the client watchlist information:

```
(Cisco Controller) >show watchlist  
client watchlist state is disabled
```