System Management Commands

clear acl counters

To clear the current counters for an Access Control List (ACL), use the **clear acl counters** command.

clear acl counters *acl_name*

Syntax Description

acl_name	ACL name.

Command Default

None

Command History

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

The following example shows how to clear the current counters for acl1:

```
(Cisco Controller) >clear acl counters acl1
```

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

ap_name	Access point name.

Command Default

None

Command History

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

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

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.
ap_mac	Access point MAC address.

Command Default

None

Command History

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

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

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

clear arp

To clear the Address Resolution Protocol (ARP) table, use the **clear arp** command.

clear arp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear the ARP table:

```
(Cisco Controller) >clear arp
Are you sure you want to clear the ARP cache? (y/n)
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear avc statistics

To clear Application Visibility and Control (AVC) statistics of a client, guest LAN, remote LAN, or a WLAN use the **clear avc statistics** command.

clear avc statistics {**client** {**all** | *client-mac*} | **guest-lan** {**all** | *guest-lan-id*} | **remote-lan** {**all** | *remote-lan-id*} | **wlan** {**all** | *wlan-id*}}

Syntax Description

client	Clears AVC statistics of a client.
all	Clears AVC statistics of all clients.
client-mac	MAC address of a client.
guest-lan	Clears AVC statistics of a guest LAN.
all	Clears AVC statistics of all guest LANs.
guest-lan-id	Guest LAN Identifier between 1 and 5.
remote-lan	Clears AVC statistics of a remote LAN.
all	Clears AVC statistics of all remote LANs.
remote-lan-id	Remote LAN Identifier between 1 and 512.
wlan	Clears AVC statistics of a WLAN.
all	Clears AVC statistics of all WLANs.
wlan-id	WLAN Identifier between 1 and 512.

Command Default

None

Command History

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

The following example shows how to clear the AVC statistics of a client:

```
(Cisco Controller) >clear avc statistics client 00:21:1b:ea:36:60
```

Related Commands

config avc profile create

config avc profile delete

config avc profile rule

config wlan avc

show avc profile

show avc applications

show avc statistics

debug avc error

debug avc events

clear client tsm

To clear the Traffic Stream Metrics (TSM) statistics for a particular access point or all the access points to which this client is associated, use the **clear client tsm** command.

clear client tsm {**802.11a** | **802.11b**} *client_mac* {*ap_mac* | **all**}

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
client_mac	MAC address of the client.
ap_mac	MAC address of a Cisco lightweight access point.
all	Specifies all access points.

Command Default

None

Command History

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

The following example shows how to clear the TSM for the MAC address 00:40:96:a8:f7:98:

```
(Cisco Controller) >clear client tsm 802.11a 00:40:96:a8:f7:98 all
```

Related Commands

clear upload start

clear config

To reset configuration data to factory defaults, use the **clear config** command.

clear config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to reset the configuration data to factory defaults:

```
(Cisco Controller) >clear config
Are you sure you want to clear the configuration? (y/n)
n
Configuration not cleared!
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear ext-webauth-url

To clear the external web authentication URL, use the **clear ext-webauth-url** command.

clear ext-webauth-url

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear the external web authentication URL:

```
(Cisco Controller) >clear ext-webauth-url
URL cleared.
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear license agent

To clear the license agent's counter or session statistics, use the **clear license agent** command.

clear license agent {**counters** | **sessions**}

Syntax Description

counters	Clears the counter statistics.
sessions	Clears the session statistics.

Command Default

None

Command History

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

The following example shows how to clear the license agent's counter settings:

```
(Cisco Controller) > clear license agent counters
```

Related Commands

config license agent

show license agent

license install

clear location rfid

To clear a specific Radio Frequency Identification (RFID) tag or all of the RFID tags in the entire database, use the **clear location rfid** command.

clear location rfid {*mac_address* | **all**}

Syntax Description

mac_address	MAC address of a specific RFID tag.
all	Specifies all the RFID tags in the database.

Command Default

None

Command History

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

The following example shows how to clear all the RFID tags in the database:

```
(Cisco Controller) >clear location rfid all
```

Related Commands

clear location statistics rfid

config location

show location

show location statistics rfid

clear location statistics rfid

To clear Radio Frequency Identification (RFID) statistics, use the **clear location statistics rfid** command.

clear location statistics rfid

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear RFID statistics:

```
(Cisco Controller) >clear location statistics rfid
```

Related Commands

config location

show location

show location statistics rfid

clear locp statistics

To clear the Location Protocol (LOCP) statistics, use the **clear locp statistics** command.

clear locp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear the statistics related to LOCP:

```
(Cisco Controller) >clear locp statistics
```

Related Commands

clear nmsp statistics

config nmsp notify-interval measurement

show nmsp notify-interval summary

show nmsp statistics

show nmsp status

clear login-banner

To remove the login banner file from the controller, use the **clear login-banner** command.

clear login-banner

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear the login banner file:

```
(Cisco Controller) >clear login-banner
```

Related Commands

transfer download datatype

clear lwapp private-config

To clear (reset to default values) an access point's current Lightweight Access Point Protocol (LWAPP) private configuration, which contains static IP addressing and controller IP address configurations, use the **clear lwapp private-config** command.

clear lwapp private-config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

Usage Guidelines

Enter the command on the access point console port.

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 Cisco WLC) 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 Access Point IOS Release 12.3(11)JX1 or later releases.

The following example shows how to clear an access point's current LWAPP private configuration:

```
ap_console >clear lwapp private-config
removing the reap config file flash:/lwapp_reap.cfg
```

clear mdns service-database

To clear the multicast DNS service database, use the **clear mdns service-database** command.

clear mdns service-database {**all** | *service-name*}

Syntax Description

all	Clears the mDNS service database.
service-name	Name of the mDNS service. The Cisco WLC clears the details of the mDNS service.

Command Default

None

Command History

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

Usage Guidelines

The Cisco WLC snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database.

The following example shows how to clear the mDNS service database:

```
(Cisco Controller) >clear mdns service-database all
```

Related Commands

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

config mdns profile

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

clear nmsp statistics

To clear the Network Mobility Services Protocol (NMSP) statistics, use the **clear nmsp statistics** command.

clear nmsp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to delete the NMSP statistics log file:

```
(Cisco Controller) >clear nmsp statistics
```

Related Commands

clear locp statistics

config nmsp notify-interval measurement

show nmsp notify-interval summary

show nmsp status

clear radius acct statistics

To clear the RADIUS accounting statistics on the controller, use the **clear radius acc statistics** command.

clear radius acct statistics [**index** | **all**]

Syntax Description

index	(Optional) Specifies the index of the RADIUS accounting server.
all	(Optional) Specifies all RADIUS accounting servers.

Command Default

None

Command History

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

The following example shows how to clear the RADIUS accounting statistics:

```
(Cisco Controller) >clear radius acc statistics
```

Related Commands

show radius acct statistics

clear tacacs auth statistics

To clear the RADIUS authentication server statistics in the controller, use the **clear tacacs auth statistics** command.

clear tacacs auth statistics [**index** | **all**]

Syntax Description

index	(Optional) Specifies the index of the RADIUS authentication server.
all	(Optional) Specifies all RADIUS authentication servers.

Command Default

None

Command History

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

The following example shows how to clear the RADIUS authentication server statistics:

```
(Cisco Controller) >clear tacacs auth statistics
```

Related Commands

show tacacs auth statistics

show tacacs summary

config tacacs auth

clear redirect-url

To clear the custom web authentication redirect URL on the Cisco Wireless LAN Controller, use the **clear redirect-url** command.

clear redirect-url

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear the custom web authentication redirect URL:

```
(Cisco Controller) >clear redirect-url
URL cleared.
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats ap wlan

To clear the WLAN statistics, use the **clear stats ap wlan** command.

clear stats ap wlan *cisco_ap*

Syntax Description

cisco_ap	Selected configuration elements.

Command Default

None

Command History

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

The following example shows how to clear the WLAN configuration elements of the access point cisco_ap:

```
(Cisco Controller) >clear stats ap wlan cisco_ap
WLAN statistics cleared.
```

clear stats local-auth

To clear the local Extensible Authentication Protocol (EAP) statistics, use the **clear stats local-auth** command.

clear stats local-auth

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear the local EAP statistics:

```
(Cisco Controller) >clear stats local-auth
Local EAP Authentication Stats Cleared.
```

Related Commands

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

clear stats mobility

To clear mobility manager statistics, use the **clear stats mobility** command.

clear stats mobility

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear mobility manager statistics:

```
(Cisco Controller) >clear stats mobility

   Mobility stats cleared.
```

clear stats port

To clear statistics counters for a specific port, use the **clear stats port** command.

clear stats port *port*

Syntax Description

port	Physical interface port number.

Command Default

None

Command History

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

The following example shows how to clear the statistics counters for port 9:

```
(Cisco Controller) >clear stats port 9
```

Related Commands

clear transfer

clear download datatype

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear stats radius

To clear the statistics for one or more RADIUS servers, use the **clear stats radius** command.

clear stats radius {**auth** | **acct**} {**index** | **all**}

Syntax Description

auth	Clears statistics regarding authentication.
acct	Clears statistics regarding accounting.
index	Specifies the index number of the RADIUS server to be cleared.
all	Clears statistics for all RADIUS servers.

Command Default

None

Command History

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

The following example shows how to clear the statistics for all RADIUS authentication servers:

```
(Cisco Controller) >clear stats radius auth all
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear stats switch

To clear all switch statistics counters on a Cisco wireless LAN controller, use the **clear stats switch** command.

clear stats switch

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear all switch statistics counters:

```
(Cisco Controller) >clear stats switch
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats tacacs

To clear the TACACS+ server statistics on the controller, use the **clear stats tacacs** command.

clear stats tacacs [**auth** | **athr** | **acct**] [**index** | **all**]

Syntax Description

auth	(Optional) Clears the TACACS+ authentication server statistics.
athr	(Optional) Clears the TACACS+ authorization server statistics.
acct	(Optional) Clears the TACACS+ accounting server statistics.
index	(Optional) Specifies index of the TACACS+ server.
all	(Optional) Specifies all TACACS+ servers.

Command Default

None

Command History

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

The following example shows how to clear the TACACS+ accounting server statistics for index 1:

```
(Cisco Controller) >clear stats tacacs acct 1
```

Related Commands

show tacacs summary

clear transfer

To clear the transfer information, use the **clear transfer** command.

clear transfer

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear the transfer information:

```
(Cisco Controller) >clear transfer
Are you sure you want to clear the transfer information? (y/n) y
Transfer Information Cleared.
```

Related Commands

transfer upload datatype

transfer upload pac

transfer upload password

transfer upload port

transfer upload path

transfer upload username

transfer upload datatype

transfer upload serverip

transfer upload start

clear traplog

To clear the trap log, use the **clear traplog** command.

clear traplog

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear the trap log:

```
(Cisco Controller) >clear traplog
Are you sure you want to clear the trap log? (y/n) y
Trap Log Cleared.
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download serverip

clear download start

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear webimage

To clear the custom web authentication image, use the **clear webimage** command.

clear webimage

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear the custom web authentication image:

```
(Cisco Controller) >clear webimage
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download serverip

clear download start

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear webmessage

To clear the custom web authentication message, use the **clear webmessage** command.

clear webmessage

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear the custom web authentication message:

```
(Cisco Controller) >clear webmessage
Message cleared.
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download serverip

clear download start

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear webtitle

To clear the custom web authentication title, use the **clear webtitle** command.

clear webtitle

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to clear the custom web authentication title:

```
(Cisco Controller) >clear webtitle
Title cleared.
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download serverip

clear download start

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

config 802.11h channelswitch

To configure an 802.11h channel switch announcement, use the **config 802.11h channelswitch** command.

config 802.11h channelswitch {**enable** {**loud** | **quiet**} | **disable**}

Syntax Description

enable	Enables the 802.11h channel switch announcement.
disable	Disables the 802.11h channel switch announcement.

Command Default

None

Command History

Release	Modification
7.6	• This command was introduced in a release earlier than Release 7.6. • The **loud** and **quiet** parameters were introduced.

The following example shows how to disable an 802.11h switch announcement:

```
(Cisco Controller) >config 802.11h channelswitch disable
```

config 802.11h powerconstraint

To configure the 802.11h power constraint value, use the **config 802.11h powerconstraint** command.

config 802.11h powerconstraint *value*

Syntax Description

value	802.11h power constraint value.

Command Default

None

Command History

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

The following example shows how to configure the 802.11h power constraint to 5:

```
(Cisco Controller) >config 802.11h powerconstraint 5
```

config 802.11h setchannel

To configure a new channel using 802.11h channel announcement, use the **config 802.11h setchannel** command.

config 802.11h setchannel *cisco_ap*

Syntax Description

cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

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

The following example shows how to configure a new channel using the 802.11h channel:

```
(Cisco Controller) >config 802.11h setchannel ap02
```

config 802.11 11nsupport

To enable 802.11n support on the network, use the **config 802.11 11nsupport** command.

config 802.11 {**a** | **b**} **11nsupport** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network settings.
b	Specifies the 802.11b/g network settings.
enable	Enables the 802.11n support.
disable	Disables the 802.11n support.

Command Default

None

Command History

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

The following example shows how to enable the 802.11n support on an 802.11a network:

```
(Cisco Controller) >config 802.11a 11nsupport enable
```

config 802.11 11nsupport a-mpdu tx priority

To specify the aggregation method used for 802.11n packets, use the **config 802.11 11nsupport a-mpdu tx priority** command.

config 802.11 {**a** | **b**} **11nsupport a-mpdu tx priority** {**0-7** | **all**} {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
0-7	Specifies the aggregated MAC protocol data unit priority level between 0 through 7.
all	Configures all of the priority levels at once.
enable	Specifies the traffic associated with the priority level uses A-MPDU transmission.
disable	Specifies the traffic associated with the priority level uses A-MSDU transmission.

Command Default

Priority 0 is enabled.

Usage Guidelines

Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). A-MPDU is performed in the software whereas A-MSDU is performed in the hardware.

Aggregated MAC Protocol Data Unit priority levels assigned per traffic type are as follows:

- 1—Background
- 2—Spare
- 0—Best effort
- 3—Excellent effort
- 4—Controlled load
- 5—Video, less than 100-ms latency and jitter
- 6—Voice, less than 10-ms latency and jitter
- 7—Network control
- all—Configure all of the priority levels at once.

Note Configure the priority levels to match the aggregation method used by the clients.

Command History

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

The following example shows how to configure all the priority levels at once so that the traffic associated with the priority level uses A-MSDU transmission:

```
(Cisco Controller) >config 802.11a 11nsupport a-mpdu tx priority all enable
```

config 802.11 11nsupport a-mpdu tx scheduler

To configure the 802.11n-5 GHz A-MPDU transmit aggregation scheduler, use the **config 802.11 11nsupport a-mpdu tx scheduler** command.

config 802.11 {**a** | **b**} **11nsupport a-mpdu tx scheduler** {**enable** | **disable** | **timeout rt** *timeout-value*}

Syntax Description

enable	Enables the 802.11n-5 GHz A-MPDU transmit aggregation scheduler.
disable	Disables the 802.11n-5 GHz A-MPDU transmit aggregation scheduler.
timeout rt	Configures the A-MPDU transmit aggregation scheduler realtime traffic timeout.
timeout-value	Timeout value in milliseconds. The valid range is between 1 millisecond to 1000 milliseconds.

Command Default

None

Usage Guidelines

Ensure that the 802.11 network is disabled before you enter this command.

Command History

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

The following example shows how to configure the A-MPDU transmit aggregation scheduler realtime traffic timeout of 100 milliseconds:

```
(Cisco Controller) >config 802.11 11nsupport a-mpdu tx scheduler timeout rt 100
```

config 802.11 11nsupport antenna

To configure an access point to use a specific antenna, use the **config 802.11 11nsupport antenna** command.

config 802.11{**a** | **b**} **11nsupport antenna** *cisco_ap* {**A** | **B** | **C** | **D**} {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a/n network.
b	Specifies the 802.11b/g/n network.
cisco_ap	Access point.
A/B/C/D	Specifies an antenna port.
enable	Enables the configuration.
disable	Disables the configuration.

Command Default

None

Command History

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

The following example shows how to configure transmission to a single antenna for legacy orthogonal frequency-division multiplexing:

```
(Cisco Controller) >config 802.11 11nsupport antenna AP1 C enable
```

config 802.11 11nsupport guard-interval

To configure the guard interval, use the **config 802.11 11nsupport guard-interval** command.

config 802.11 {**a** | **b**} **11nsupport guard-interval** {**any** | **long**}

Syntax Description

any	Enables either a short or a long guard interval.
long	Enables only a long guard interval.

Command Default

None

Command History

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

The following example shows how to configure a long guard interval:

```
(Cisco Controller) >config 802.11 11nsupport guard-interval long
```

config 802.11 11nsupport mcs tx

To specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client, use the **config 802.11 11nsupport mcs tx** command.

config 802.11 {**a** | **b**} **11nsupport mcs tx** {**0-15**} {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
11nsupport	Specifies support for 802.11n devices.
mcs tx	Specifies the modulation and coding scheme data rates as follows: • 0 (7 Mbps) • 1 (14 Mbps) • 2 (21 Mbps) • 3 (29 Mbps) • 4 (43 Mbps) • 5 (58 Mbps) • 6 (65 Mbps) • 7 (72 Mbps) • 8 (14 Mbps) • 9 (29 Mbps) • 10 (43 Mbps) • 11 (58 Mbps) • 12 (87 Mbps) • 13 (116 Mbps) • 14 (130 Mbps) • 15 (144 Mbps)
enable	Enables this configuration.
disable	Disables this configuration.

Command Default

None

Command History

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

The following example shows how to specify MCS rates:

```
(Cisco Controller) >config 802.11a 11nsupport mcs tx 5 enable
```

config 802.11 11nsupport rifs

To configure the Reduced Interframe Space (RIFS) between data frames and its acknowledgment, use the **config 802.11 11nsupport rifs** command.

config 802.11 {**a** | **b**} **11nsupport rifs** {**enable** | **disable**}

Syntax Description

enable	Enables RIFS for the 802.11 network.
disable	Disables RIFS for the 802.11 network.

Command Default

None

Command History

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

This example shows how to enable RIFS:

```
(Cisco Controller) >config 802.11a 11nsupport rifs enable
```

Related Topics

config 802.11-a

config 802.11 beacon period

To change the beacon period globally for an 802.11a, 802.11b, or other supported 802.11 network, use the **config 802.11 beacon period** command.

config 802.11 {**a** | **b**} **beacon period** *time_units*

Note Disable the 802.11 network before using this command. See the "Usage Guidelines" section.

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
time_units	Beacon interval in time units (TU). One TU is 1024 microseconds.

Command Default

None

Usage Guidelines

In Cisco wireless LAN solution 802.11 networks, all Cisco lightweight access point wireless LANs broadcast a beacon at regular intervals. This beacon notifies clients that the 802.11a service is available and allows the clients to synchronize with the lightweight access point.

Before you change the beacon period, make sure that you have disabled the 802.11 network by using the **config 802.11 disable** command. After changing the beacon period, enable the 802.11 network by using the **config 802.11 enable** command.

Command History

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

This example shows how to configure an 802.11a network for a beacon period of 120 time units:

```
(Cisco Controller) > config 802.11 beacon period 120
```

Related Commands

show 802.11a

config 802.11b beaconperiod

config 802.11a disable

config 802.11a enable

config 802.11 cac defaults

To configure the default Call Admission Control (CAC) parameters for the 802.11a and 802.11b/g network, use the **config 802.11 cac defaults** command.

config 802.11 {**a** | **b**} **cac defaults**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Usage Guidelines

CAC commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

This example shows how to configure the default CAC parameters for the 802.11a network:

```
(Cisco Controller) > config 802.11 cac defaults
```

Related Commands

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video sip

config 802.11 cac video roam-bandwidth

config 802.11 cac load-based

config 802.11 cac media-stream

config 802.11 cac multimedia

config 802.11 cac video cac-method

debug cac

config 802.11 cac video acm

To enable or disable video Call Admission Control (CAC) for the 802.11a or 802.11b/g network, use the **config 802.11 cac video acm** command.

config 802.11 {**a** | **b**} **cac video acm** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables video CAC settings.
disable	Disables video CAC settings.

Command Default

The default video CAC settings for the 802.11a or 802.11b/g network is disabled.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable**, or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to enable the video CAC for the 802.11a network:

```
(Cisco Controller) > config 802.11 cac video acm enable
```

The following example shows how to disable the video CAC for the 802.11b network:

```
(Cisco Controller) > config 802.11 cac video acm disable
```

Related Commands

config 802.11 cac video max-bandwidth

config 802.11 cac video roam-bandwidth

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video cac-method

To configure the Call Admission Control (CAC) method for video applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac video cac-method** command.

config 802.11 {**a** | **b**} **cac video cac-method** {**static** | **load-based**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
static	Enables the static CAC method for video applications on the 802.11a or 802.11b/g network. Static or bandwidth-based CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new video request and in turn enables the access point to determine whether it is capable of accommodating the request.
load-based	Enables the load-based CAC method for video applications on the 802.11a or 802.11b/g network. Load-based or dynamic CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by collocated channel interference. Load-based CAC also covers the additional bandwidth consumption results from PHY and channel impairment. The access point admits a new call only if the channel has enough unused bandwidth to support that call. Load-based CAC is not supported if SIP-CAC is enabled.

Command Default

Static.

Usage Guidelines

CAC commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Video CAC consists of two parts: Unicast Video-CAC and MC2UC CAC. If you need only Unicast Video-CAC, you must configure only static mode. If you need only MC2UC CAC, you must configure Static or Load-based CAC. Load-based CAC is not supported if SIP-CAC is enabled.

Command History

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

This example shows how to enable the static CAC method for video applications on the 802.11a network:

```
(Cisco Controller) > config 802.11 cac video cac-method static
```

Related Commands

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video sip

config 802.11 cac video roam-bandwidth

config 802.11 cac load-based

config 802.11 cac defaults

config 802.11 cac media-stream

config 802.11 cac multimedia

debug cac

config 802.11 cac video load-based

To enable or disable load-based Call Admission Control (CAC) for video applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac video load-based** command.

config 802.11 {**a** | **b**} **cac video load-based** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables load-based CAC for video applications on the 802.11a or 802.11b/g network. Load-based or dynamic CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by collocated channel interference. Load-based CAC also covers the additional bandwidth consumption results from PHY and channel impairment. The access point admits a new call only if the channel has enough unused bandwidth to support that call.
disable	Disables load-based CAC method for video applications on the 802.11a or 802.11b/g network.

Command Default

Disabled.

Usage Guidelines

CAC commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Video CAC consists of two parts: Unicast Video-CAC and MC2UC CAC. If you need only Unicast Video-CAC, you must configure only static mode. If you need only MC2UC CAC, you must configure Static or Load-based CAC. Load-based CAC is not supported if SIP-CAC is enabled.

Note Load-based CAC is not supported if SIP-CAC is enabled.

Command History

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

This example shows how to enable load-based CAC method for video applications on the 802.11a network:

```
(Cisco Controller) > config 802.11 cac video load-based enable
```

Related Commands

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video sip

config 802.11 cac video roam-bandwidth

config 802.11 cac load-based

config 802.11 cac defaults

config 802.11 cac media-stream

config 802.11 cac multimedia

config 802.11 cac video cac-method

debug cac

config 802.11 cac video max-bandwidth

To set the percentage of the maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac video max-bandwidth** command.

config 802.11 {**a** | **b**} **cac video max-bandwidth** *bandwidth*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
bandwidth	Bandwidth percentage value from 5 to 85%.

Command Default

The default maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network is 0%.

Usage Guidelines

The maximum radio frequency (RF) bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network.

Note If this parameter is set to zero (0), the controller assumes that you do not want to allocate any bandwidth and allows all bandwidth requests.

Call Admission Control (CAC) commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable**, or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to specify the percentage of the maximum allocated bandwidth for video applications on the selected radio band:

```
(Cisco Controller) > config 802.11 cac video max-bandwidth 50
```

Related Commands

config 802.11 cac video acm

config 802.11 cac video roam-bandwidth

config 802.11 cac voice stream-size

config 802.11 cac voice roam-bandwidth

config 802.11 cac media-stream

To configure media stream Call Admission Control (CAC) voice and video quality parameters for 802.11a and 802.11b networks, use the **config 802.11 cac media-stream** command.

config 802.11 {**a** | **b**} **cac media-stream multicast-direct** {**max-retry-percent** *retry-percentage* | **min-client-rate** *dot11-rate*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
multicast-direct	Configures CAC parameters for multicast-direct media streams.
max-retry-percent	Configures the percentage of maximum retries that are allowed for multicast-direct media streams.
retry-percentage	Percentage of maximum retries that are allowed for multicast-direct media streams.
min-client-rate	Configures the minimum transmission data rate to the client for multicast-direct media streams.
dot11-rate	Minimum transmission data rate to the client for multicast-direct media streams. Rate in kbps at which the client can operate. If the transmission data rate is below this rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial. The available data rates are 6000, 9000, 12000, 18000, 24000, 36000, 48000, 54000, and 11n rates.

Command Default

The default value for the maximum retry percent is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video will be demoted for better effort QoS or is subject to denial.

Usage Guidelines

CAC commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to configure the maximum retry percent for multicast-direct media streams as 90 on a 802.11a network:

```
(Cisco Controller) > config 802.11 cac media-stream multicast-direct max-retry-percent 90
```

Related Commands

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video sip

config 802.11 cac video roam-bandwidth

config 802.11 cac load-based

config 802.11 cac defaults

config 802.11 cac multimedia

debug cac

config 802.11 cac multimedia

To configure the CAC media voice and video quality parameters for 802.11a and 802.11b networks, use the **config 802.11 cac multimedia** command.

config 802.11 {**a** | **b**} **cac multimedia max-bandwidth** *bandwidth*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
max-bandwidth	Configures the percentage of maximum bandwidth allocated to Wi-Fi Multimedia (WMM) clients for voice and video applications on the 802.11a or 802.11b/g network.
bandwidth	Percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 802.11a or 802.11b/g network. Once the client reaches the specified value, the access point rejects new calls on this radio band. The range is from 5 to 85%.

Command Default

The default maximum bandwidth allocated to Wi-Fi Multimedia (WMM) clients for voice and video applications on the 802.11a or 802.11b/g network is 85%.

Usage Guidelines

Call Admission Control (CAC) commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to configure the percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 802.11a network:

```
(Cisco Controller) > config 802.11 cac multimedia max-bandwidth 80
```

Related Commands

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video sip

config 802.11 cac video roam-bandwidth

config 802.11 cac load-based

config 802.11 cac defaults

debug cac

config 802.11 cac video roam-bandwidth

To configure the percentage of the maximum allocated bandwidth reserved for roaming video clients on the 802.11a or 802.11b/g network, use the **config 802.11 cac video roam-bandwidth** command.

config 802.11 {**a** | **b**} **cac video roam-bandwidth** *bandwidth*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
bandwidth	Bandwidth percentage value from 5 to 85%.

Command Default

The maximum allocated bandwidth reserved for roaming video clients on the 802.11a or 802.11b/g network is 0%.

Command History

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

Usage Guidelines

The controller reserves the specified bandwidth from the maximum allocated bandwidth for roaming video clients.

Note If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests.

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

The following example shows how to specify the percentage of the maximum allocated bandwidth reserved for roaming video clients on the selected radio band:

```
(Cisco Controller) > config 802.11 cac video roam-bandwidth 10
```

Related Commands

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video cac-method

config 802.11 cac video sip

config 802.11 cac video load-based

config 802.11 cac video sip

To enable or disable video Call Admission Control (CAC) for nontraffic specifications (TSPEC) SIP clients using video applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac video sip** command.

config 802.11 {**a** | **b**} **cac video sip** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables video CAC for non-TSPEC SIP clients using video applications on the 802.11a or 802.11b/g network. When you enable video CAC for non-TSPEC SIP clients, you can use applications like Facetime and CIUS video calls.
disable	Disables video CAC for non-TSPEC SIP clients using video applications on the 802.11a or 802.11b/g network.

Command Default

None

Usage Guidelines

CAC commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.
- Enable call snooping on the WLAN on which the SIP client is present by entering the **config wlan call-snoop enable** *wlan_id* command.

The following example shows how to enable video CAC for non-TSPEC SIP clients using video applications on the 802.11a network:

```
(Cisco Controller) > config 802.11 cac video sip enable
```

Related Commands

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video cac-method

config 802.11 cac video load-based

config 802.11 cac video roam-bandwidth

config 802.11 cac video tspec-inactivity-timeout

To process or ignore the Call Admission Control (CAC) Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point, use the **config 802.11 cac video tspec-inactivity-timeout** command.

config 802.11 {**a** | **b**} **cac video tspec-inactivity-timeout** {**enable** | **ignore**}

Syntax Description

a	Specifies the 802.11a network.
ab	Specifies the 802.11b/g network.
enable	Processes the TSPEC inactivity timeout messages.
ignore	Ignores the TSPEC inactivity timeout messages.

Command Default

The default CAC WMM TSPEC inactivity timeout received from an access point is disabled (ignore).

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

This example shows how to process the response to TSPEC inactivity timeout messages received from an access point:

```
(Cisco Controller) > config 802.11a cac video tspec-inactivity-timeout enable
```

This example shows how to ignore the response to TSPEC inactivity timeout messages received from an access point:

```
(Cisco Controller) > config 802.11a cac video tspec-inactivity-timeout ignore
```

Related Commands

config 802.11 cac video acm

config 802.11 cac video max-bandwidth

config 802.11 cac video roam-bandwidth

config 802.11 cac voice acm

To enable or disable bandwidth-based voice Call Admission Control (CAC) for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice acm** command.

config 802.11 {**a** | **b**} **cac voice acm** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the bandwidth-based CAC.
disable	Disables the bandwidth-based CAC.

Command Default

The default bandwidth-based voice CAC for the 802.11a or 802.11b/g network id disabled.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

This example shows how to enable the bandwidth-based CAC:

```
(Cisco Controller) > config 802.11c cac voice acm enable
```

This example shows how to disable the bandwidth-based CAC:

```
(Cisco Controller) > config 802.11b cac voice acm disable
```

Related Commands

config 802.11 cac video acm

config 802.11 cac voice max-bandwidth

To set the percentage of the maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac voice max-bandwidth** command.

config 802.11 {**a** | **b**} **cac voice max-bandwidth** *bandwidth*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
bandwidth	Bandwidth percentage value from 5 to 85%.

Command Default

The default maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network is 0%.

Usage Guidelines

The maximum radio frequency (RF) bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network.

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to specify the percentage of the maximum allocated bandwidth for voice applications on the selected radio band:

```
(Cisco Controller) > config 802.11a cac voice max-bandwidth 50
```

Related Commands

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice stream-size

config 802.11 exp-bwreq

config 802.11 tsm

config wlan save

show wlan

show wlan summary

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 cac voice load-based

config 802.11 cac video acm

config 802.11 cac voice roam-bandwidth

To configure the percentage of the Call Admission Control (CAC) maximum allocated bandwidth reserved for roaming voice clients on the 802.11a or 802.11b/g network, use the **config 802.11 cac voice roam-bandwidth** command.

config 802.11 {**a** | **b**} **cac voice roam-bandwidth** *bandwidth*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
bandwidth	Bandwidth percentage value from 0 to 85%.

Command Default

The default CAC maximum allocated bandwidth reserved for roaming voice clients on the 802.11a or 802.11b/g network is 85%.

Usage Guidelines

The maximum radio frequency (RF) bandwidth cannot exceed 85% for voice and video. The controller reserves the specified bandwidth from the maximum allocated bandwidth for roaming voice clients.

Note If this parameter is set to zero (0), the controller assumes you do not want to allocate any bandwidth and therefore allows all bandwidth requests.

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to configure the percentage of the maximum allocated bandwidth reserved for roaming voice clients on the selected radio band:

```
(Cisco Controller) > config 802.11 cac voice roam-bandwidth 10
```

Related Commands

config 802.11 cac voice acm

config 802.11cac voice max-bandwidth

config 802.11 cac voice stream-size

config 802.11 cac voice tspec-inactivity-timeout

To process or ignore the Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point, use the **config 802.11 cac voice tspec-inactivity-timeout** command.

config 802.11 {**a** | **b**} **cac voice tspec-inactivity-timeout** {**enable** | **ignore**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Processes the TSPEC inactivity timeout messages.
ignore	Ignores the TSPEC inactivity timeout messages.

Command Default

The default WMM TSPEC inactivity timeout received from an access point is disabled (ignore).

Usage Guidelines

Call Admission Control (CAC) commands require that the WLAN you are planning to modify is configured for Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to enable the voice TSPEC inactivity timeout messages received from an access point:

```
(Cisco Controller) > config 802.11 cac voice tspec-inactivity-timeout enable
```

Related Commands

config 802.11 cac voice load-based

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice acm

config 802.11cac voice max-bandwidth

config 802.11 cac voice stream-size

config 802.11 cac voice load-based

To enable or disable load-based Call Admission Control (CAC) for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice load-based** command.

config 802.11 {**a** | **b**} **cac voice load-based** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables load-based CAC.
disable	Disables load-based CAC.

Command Default

The default load-based CAC for the 802.11a or 802.11b/g network is disabled.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id command*.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to enable the voice load-based CAC parameters:

```
(Cisco Controller) > config 802.11a cac voice load-based enable
```

The following example shows how to disable the voice load-based CAC parameters:

```
(Cisco Controller) > config 802.11a cac voice load-based disable
```

Related Commands

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac voice stream-size

config 802.11 cac voice max-calls

Note Do not use the **config 802.11 cac voice max-calls** command if the SIP call snooping feature is disabled and if the SIP based Call Admission Control (CAC) requirements are not met.

To configure the maximum number of voice call supported by the radio, use the **config 802.11 cac voice max-calls** command.

config 802.11 {**a** | **b**} **cac voice max-calls** *number*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
number	Number of calls to be allowed per radio.

Command Default

The default maximum number of voice call supported by the radio is 0, which means that there is no maximum limit check for the number of calls.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id command*.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to configure the maximum number of voice calls supported by radio:

```
(Cisco Controller) > config 802.11 cac voice max-calls 10
```

Related Commands

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice stream-size

config 802.11 exp-bwreq

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 cac voice load-based

config 802.11 cac video acm

config 802.11 cac voice sip bandwidth

Note SIP bandwidth and sample intervals are used to compute per call bandwidth for the SIP-based Call Admission Control (CAC).

To configure the bandwidth that is required per call for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice sip bandwidth** command.

config 802.11 {**a** | **b**} **cac voice sip bandwidth** *bw_kbps* **sample-interval** *number_msecs*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
bw_kbps	Bandwidth in kbps.
sample-interval	Specifies the packetization interval for SIP codec.
number_msecs	Packetization sample interval in msecs. The sample interval for SIP codec is 20 seconds.

Command Default

None

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable** network command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to configure the bandwidth and voice packetization interval for a SIP codec:

```
(Cisco Controller) > config 802.11 cac voice sip bandwidth 10 sample-interval 40
```

Related Commands

config 802.11 cac voice acm

config 802.11 cac voice load-based

config 802.11 cac voice max-bandwidth

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 exp-bwreq

config 802.11 cac voice sip codec

To configure the Call Admission Control (CAC) codec name and sample interval as parameters and to calculate the required bandwidth per call for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice sip codec** command.

config 802.11 {**a** | **b**} **cac voice sip codec** {**g711** | **g729**} **sample-interval** *number_msecs*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
g711	Specifies CAC parameters for the SIP G711 codec.
g729	Specifies CAC parameters for the SIP G729 codec.
sample-interval	Specifies the packetization interval for SIP codec.
number_msecs	Packetization interval in msecs. The sample interval for SIP codec value is 20 seconds.

Command Default

The default CAC codec parameter is g711.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable** network command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to configure the codec name and sample interval as parameters for SIP G711 codec:

```
(Cisco Controller) >  config 802.11a cac voice sip codec g711 sample-interval 40
```

This example shows how to configure the codec name and sample interval as parameters for SIP G729 codec:

```
(Cisco Controller) > config 802.11a cac voice sip codec g729 sample-interval 40
```

Related Commands

config 802.11 cac voice acm

config 802.11 cac voice load-based

config 802.11 cac voice max-bandwidth

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 exp-bwreq

config 802.11 cac voice stream-size

To configure the number of aggregated voice Wi-Fi Multimedia (WMM) traffic specification (TSPEC) streams at a specified data rate for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice stream-size** command.

config 802.11 {**a** | **b**} **cac voice stream-size** *stream_size number* **mean_datarate max-streams** *mean_datarate*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
stream-size	Configures the maximum data rate for the stream.
stream_size	Range of stream size is between 84000 and 92100.
number	Number (1 to 5) of voice streams.
mean_datarate	Configures the mean data rate.
max-streams	Configures the mean data rate of a voice stream.
mean_datarate	Mean data rate (84 to 91.2 kbps) of a voice stream.

Command Default

The default number of streams is 2 and the mean data rate of a stream is 84 kbps.

Usage Guidelines

Call Admission Control (CAC) commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable** network command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to configure the number of aggregated voice traffic specifications stream with the stream size 5 and the mean data rate of 85000 kbps:

```
(Cisco Controller) > config 802.11 cac voice stream-size 5 max-streams size 85
```

Related Commands

config 802.11 cac voice acm

config 802.11 cac voice load-based

config 802.11 cac voice max-bandwidth

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 exp-bwreq

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 radio.
b	Specifies the 802.11b/g network.
network	Disables transmission for the entire 802.11a network.
cisco_ap	Individual Cisco lightweight access point radio.

Command Default

The transmission is enabled for the entire network by default.

Command History

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

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 802.11 dtpc

To enable or disable the Dynamic Transmit Power Control (DTPC) setting for an 802.11 network, use the **config 802.11 dtpc** command.

config 802.11 {**a** | **b**} **dtpc** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the support for this command.
disable	Disables the support for this command.

Command Default

The default DTPC setting for an 802.11 network is enabled.

Command History

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

The following example shows how to disable DTPC for an 802.11a network:

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

config 802.11 enable

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

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

Syntax Description

a	Configures the 802.11a radio
b	Specifies the 802.11b/g network.
network	Disables transmission for the entire 802.11a network.
cisco_ap	Individual Cisco lightweight access point radio.

Command Default

The transmission is enabled for the entire network by default.

Usage Guidelines

Use this command with the **config 802.11 disable** command when configuring 802.11 settings.

This command can be used any time that the CLI interface is active.

Command History

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

The following example shows how to enable radio transmission for the entire 802.11a network:

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

The following example shows how to enable radio transmission for AP1 on an 802.11b network:

```
(Cisco Controller) > config 802.11b enable AP1
```

Related Commands

show sysinfo show 802.11a

config wlan radio

config 802.11a disable

config 802.11b disable

config 802.11b enable

config 802.11b 11gSupport enable

config 802.11b 11gSupport disable

config 802.11 exp-bwreq

To enable or disable the Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature for an 802.11 radio, use the **config 802.11 exp-bwreq** command.

config 802.11 {**a** | **b**} **exp-bwreq** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the expedited bandwidth request feature.
disable	Disables the expedited bandwidth request feature.

Command Default

The expedited bandwidth request feature is disabled by default.

Usage Guidelines

When this command is enabled, the controller configures all joining access points for this feature.

Command History

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

The following example shows how to enable the CCX expedited bandwidth settings:

```
(Cisco Controller) > config 802.11a exp-bwreq enable
Cannot change Exp Bw Req mode while 802.11a network is operational.
```

The following example shows how to disable the CCX expedited bandwidth settings:

```
(Cisco Controller) > config 802.11a exp-bwreq disable
```

Related Commands

show 802.11a

show ap stats 802.11a

config 802.11 fragmentation

To configure the fragmentation threshold on an 802.11 network, use the **config 802.11 fragmentation** command.

config 802.11{**a** | **b**} **fragmentation** *threshold*

Note This command can only be used when the network is disabled using the **config 802.11 disable** command.

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
threshold	Number between 256 and 2346 bytes (inclusive).

Command Default

None.

Command History

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

This example shows how to configure the fragmentation threshold on an 802.11a network with the threshold number of 6500 bytes:

```
(Cisco Controller) > config 802.11a fragmentation 6500
```

Related Commands

config 802.11b fragmentation

show 802.11b

show ap auto-rtf

config 802.11 l2roam rf-params

To configure 802.11a or 802.11b/g Layer 2 client roaming parameters, use the **config 802.11 l2roam rf-params** command.

config 802.11 {**a** | **b**} **l2roam rf-params** {**default** | **custom** *min_rssi roam_hyst scan_thresh trans_time*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
default	Restores Layer 2 client roaming RF parameters to default values.
custom	Configures custom Layer 2 client roaming RF parameters.
min_rssi	Minimum received signal strength indicator (RSSI) that is required for the client to associate to the access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. The valid range is –80 to –90 dBm, and the default value is –85 dBm.
roam_hyst	How much greater the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between the two access points. The valid range is 2 to 4 dB, and the default value is 2 dB.
scan_thresh	Minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold. The valid range is –70 to –77 dBm, and the default value is –72 dBm.

trans_time	Maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold. The valid range is 1 to 10 seconds, and the default value is 5 seconds. **Note** For high-speed client roaming applications in outdoor mesh environments, we recommend that you set the transition time to 1 second.

Command Default

The default minimum RSSI is -85 dBm. The default signal strength of a neighboring access point is 2 dB. The default scan threshold value is -72 dBm. The default time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam is 5 seconds.

Usage Guidelines

For high-speed client roaming applications in outdoor mesh environments, we recommend that you set the *trans_time* to 1 second.

Command History

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

The following example shows how to configure custom Layer 2 client roaming parameters on an 802.11a network:

```
(Cisco Controller) > config 802.11 l2roam rf-params custom –80 2 –70 7
```

Related Commands

show advanced 802.11 l2roam

show l2tp

config 802.11 max-clients

To configure the maximum number of clients per access point, use the **config 802.11 max-clients** command.

config 802.11 {**a** | **b**} **max-clients** *max-clients*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
max-clients	Configures the maximum number of client connections per access point.
max-clients	Maximum number of client connections per access point. The range is from 1 to 200.

Command Default

None

Command History

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

The following example shows how to set the maximum number of clients at 22:

```
(Cisco Controller) > config 802.11 max-clients 22
```

Related Commands

show ap config 802.11a

config 802.11b rate

config 802.11 multicast data-rate

To configure the minimum multicast data rate, use the **config 802.11 multicast data-rate** command.

config 802.11{**a** | **b**} **multicast data-rate** *data_rate* [**ap** *ap_name* | **default**]

Syntax Description

data_rate	Minimum multicast data rates. The options are 6, 9, 12, 18, 24, 36, 48, 54. Enter 0 to specify that APs will dynamically adjust the number of the buffer allocated for multicast.
ap_name	Specific AP radio in this data rate.
default	Configures all APs radio in this data rate.

Command Default

The default is 0 where the configuration is disabled and the multicast rate is the lowest mandatory data rate and unicast client data rate.

Usage Guidelines

When you configure the data rate without the AP name or **default** keyword, you globally reset all the APs to the new value and update the controller global default with this new data rate value. If you configure the data rate with **default** keyword, you only update the controller global default value and do not reset the value of the APs that are already joined to the controller. The APs that join the controller after the new data rate value is set receives the new data rate value.

Command History

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

The following example shows how to configure minimum multicast data rate settings:

```
(Cisco Controller) > config 802.11 multicast data-rate 12
```

config 802.11 rate

To set mandatory and supported operational data rates for an 802.11 network, use the **config 802.11 rate** command.

config 802.11 {**a** | **b**} **rate** {**disabled** | **mandatory** | **supported**} *rate*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
disabled	Disables a specific data rate.
mandatory	Specifies that a client supports the data rate in order to use the network.
supported	Specifies to allow any associated client that supports the data rate to use the network.
rate	Rate value of 6, 9, 12, 18, 24, 36, 48, or 54 Mbps.

Command Default

None

Usage Guidelines

The data rates set with this command are negotiated between the client and the Cisco wireless LAN controller. If the data rate is set to **mandatory**, the client must support it in order to use the network. If a data rate is set as **supported** by the Cisco wireless LAN controller, any associated client that also supports that rate may communicate with the Cisco lightweight access point using that rate. It is not required that a client is able to use all the rates marked **supported** in order to associate.

Command History

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

The following example shows how to set the 802.11b transmission at a mandatory rate at 12 Mbps:

```
(Cisco Controller) > config 802.11b rate mandatory 12
```

Related Commands

show ap config 802.11a

config 802.11b rate

config 802.11 tsm

To enable or disable the video Traffic Stream Metric (TSM) option for the 802.11a or 802.11b/g network, use the **config 802.11 tsm** command.

config 802.11 {**a** | **b**} **tsm** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the video TSM settings.
disable	Disables the video TSM settings.

Command Default

By default, the TSM for the 802.11a or 802.11b/g network is disabled.

Command History

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

The following example shows how to enable the video TSM option for the 802.11b/g network:

```
(Cisco Controller) > config 802.11b tsm enable
```

The following example shows how to disable the video TSM option for the 802.11b/g network:

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

Related Commands

show ap stats

show client tsm

config advanced 802.11 7920VSIEConfig

To configure the Cisco unified wireless IP phone 7920 VISE parameters, use the **config advanced 802.11 7920VSIEConfig** command.

config advanced 802.11 {**a** | **b**} **7920VSIEConfig** {**call-admission-limit** *limit* | **G711-CU-Quantum** *quantum*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
call-admission-limit	Configures the call admission limit for the 7920s.
G711-CU-Quantum	Configures the value supplied by the infrastructure indicating the current number of channel utilization units that would be used by a single G.711-20ms call.
limit	Call admission limit (from 0 to 255). The default value is 105.
quantum	G711 quantum value. The default value is 15.

Command Default

None

Command History

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

This example shows how to configure the call admission limit for 7920 VISE parameters:

```
(Cisco Controller) >config advanced 802.11 7920VSIEConfig call-admission-limit 4
```

config advanced 802.11 edca-parameters

To enable a specific Enhanced Distributed Channel Access (EDCA) profile on a 802.11a network, use the **config advanced 802.11 edca-parameters** command.

config advanced 802.11 {**a** | **b**} **edca-parameters** {**wmm-default** | **svp-voice** | **optimized-voice** | **optimized-video-voice** | **custom-voice** | | **custom-set** { *QoS Profile Name* } { **aifs** *AP-value (0-16) Client value (0-16)* | **ecwmax** *AP-Value (0-10) Client value (0-10)* | **ecwmin** *AP-Value (0-10) Client value (0-10)* | **txop** *AP-Value (0-255) Client value (0-255)* } }

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
wmm-default	Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option if voice or video services are not deployed on your network.
svp-voice	Enables Spectralink voice-priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls.
optimized-voice	Enables EDCA voice-optimized profile parameters. Choose this option if voice services other than Spectralink are deployed on your network.
optimized-video-voice	Enables EDCA voice-optimized and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network. **Note** If you deploy video services, admission control must be disabled.
custom-voice	Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

custom-set	Enables customization of EDCA parameters • **aifs—Configures the Arbitration Inter-Frame Space.** **AP Value (0-16) Client value (0-16)** • **ecwmax—Configures the maximum Contention Window.** **AP Value(0-10) Client Value (0-10)** • **ecwmin—Configures the minimum Contention Window.** **AP Value(0-10) Client Value(0-10)** • **txop—Configures the Arbitration Transmission Opportunity Limit.** **AP Value(0-255) Client Value(0-255)** QoS Profile Name - Enter the QoS profile name: • bronze • silver • gold • platinum

Command Default

The default EDCA parameter is **wmm-default**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.2.110.0	In this release, custom-set keyword was added to edca-parameters command.

Examples

The following example shows how to enable Spectralink voice-priority parameters:

```
(Cisco Controller) > config advanced 802.11 edca-parameters svp-voice
```

Related Commands

config advanced 802.11b edca-parameters	Enables a specific Enhanced Distributed Channel Access (EDCA) profile on the 802.11a network.
show 802.11a	Displays basic 802.11a network settings.

Related Topics

config advanced 802.11 coverage fail-rate

config advanced 802.11 channel update

config advanced fastpath fastcache

To configure the fastpath fast cache control, use the **config advanced fastpath fastcache** command.

config advanced fastpath fastcache {**enable** | **disable**}

Syntax Description

enable	Enables the fastpath fast cache control.
disable	Disables the fastpath fast cache control.

Command Default

None

Command History

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

The following example shows how to enable the fastpath fast cache control:

```
(Cisco Controller) > config advanced fastpath fastcache enable
```

Related Commands

config advanced fastpath pkt-capture

config advanced fastpath pkt-capture

To configure the fastpath packet capture, use the **config advanced fastpath pkt-capture** command.

config advanced fastpath pkt-capture {**enable** | **disable**}

Syntax Description

enable	Enables the fastpath packet capture.
disable	Disables the fastpath packet capture.

Command Default

None

Command History

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

The following example shows how to enable the fastpath packet capture:

```
(Cisco Controller) > config advanced fastpath pkt-capture enable
```

Related Commands

config advanced fastpath fastcache

config advanced sip-preferred-call-no

To configure voice prioritization, use the **config advanced sip-preferred-call-no** command.

config advanced sip-preferred-call-no *call_index* {*call_number* | **none**}

Syntax Description

call_index	Call index with valid values between 1 and 6.
call_number	Preferred call number that can contain up to 27 characters.
none	Deletes the preferred call set for the specified index.

Command Default

None

Usage Guidelines

Before you configure voice prioritization, you must complete the following prerequisites:

- Set the voice to the platinum QoS level by entering the **config wlan qos** *wlan-id* **platinum** command.
- Enable the admission control (ACM) to this radio by entering the **config 802.11** {**a** | **b**} **cac** {**voice** | **video**} **acm enable** command.
- Enable the call-snooping feature for a particular WLAN by entering the **config wlan call-snoop enable** *wlan-id* command.

  To view statistics about preferred calls, enter the **show ap stats** {**802.11**{**a** | **b**} | **wlan**} *cisco_ap* command.

Command History

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

The following example shows how to add a new preferred call for index 2:

```
(Cisco Controller) > config advanced sip-preferred-call-no 2 0123456789
```

Related Commands

config wlan qos

config 802.11 cac video acm

config 802.11 cac voice acm

config wlan call-snoop

show ap stats

config advanced sip-snooping-ports

To configure call snooping ports, use the **config advanced sip-snooping-ports** command.

config advanced sip-snooping-ports *start_port end_port*

Syntax Description

start_port	Starting port for call snooping. The range is from 0 to 65535.
end_port	Ending port for call snooping. The range is from 0 to 65535.

Usage Guidelines

If you need only a single port for call snooping, configure the start and end port with the same number.

The port used by the CIUS tablet is 5060 and the port range used by Facetime is from 16384 to16402.

Command History

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

The following example shows how to configure the call snooping ports:

```
(Cisco Controller) > config advanced sip-snooping-ports 4000 4500
```

Related Commands

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video sip

config 802.11 cac voice sip

show advanced sip-preferred-call-no

show advanced sip-snooping-ports

debug cac

config avc profile create

To create a new Application Visibility and Control (AVC) profile, use the **config avc profile create** command.

config avc profile *profile_name* **create**

Syntax Description

profile_name	Name of the AVC profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
create	Creates a new AVC profile.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs. You can configure only one AVC profile per WLAN and each AVC profile can have up to 32 rules. Each rule states a Mark or Drop action for an application, which allows you to configure up to 32 application actions per WLAN.

The following example shows how to create a new AVC profile:

```
(Cisco Controller) > config avc profile avcprofile1 create
```

Related Commands

config avc profile delete

config avc profile rule

config wlan avc

show avc profile

show avc applications

show avc statistics

debug avc error

debug avc events

config avc profile delete

To delete an Application Visibility and Control (AVC) profile, use the **config avc profile delete** command.

config avc profile *profile_name* **delete**

Syntax Description

profile_name	Name of the AVC profile.
delete	Deletes an AVC profile.

Command Default

The AVC profile is not deleted.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to delete an AVC profile:

```
(Cisco Controller) > config avc profile avcprofile1 delete
```

Related Commands

config avc profile create

config avc profile rule

config wlan avc

show avc profile summary

show avc profile detailed

debug avc error

debug avc events

config avc profile rule

To configure a rule for an Application Visibility and Control (AVC) profile, use the **config avc profile rule** command.

config avc profile *profile_name* **rule** {**add** | **remove**} **application** *application_name* {**drop** | **mark** *dscp*}

Syntax Description

profile_name	Name of the AVC profile.
rule	Configures a rule for the AVC profile.
add	Creates a rule for the AVC profile.
remove	Deletes a rule for the AVC profile.
application	Specifies the application that has to be dropped or marked.
application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
drop	Drops the upstream and downstream packets that correspond to the chosen application.
mark	Marks the upstream and downstream packets that correspond to the chosen application with the Differentiated Services Code Point (DSCP) value that you specify in the drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.
dscp	Packet header code that is used to define the QoS across the Internet. The range is from 0 to 63.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to configure a rule for an AVC profile:

```
(Cisco Controller) > config avc profile avcprofile1 rule add application gmail mark 10
```

Related Commands

config avc profile delete

config avc profile create

config wlan avc

show avc profile

show avc applications

show avc statistics

debug avc error

debug avc events

config band-select cycle-count

To set the band select probe cycle count, use the **config band-select cycle-count** command.

config band-select cycle-count *count*

Syntax Description

count	Value for the cycle count between 1 to 10.

Command Default

None

Command History

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

The following example shows how to set the probe cycle count for band select to 8:

```
(Cisco Controller) > config band-select cycle-count 8
```

Related Commands

config band-select cycle-threshold

config band-select expire

config band-select client-rssi

config band-select cycle-threshold

To set the time threshold for a new scanning cycle, use the **config band-select cycle-threshold** command.

config band-select cycle-threshold *threshold*

Syntax Description

threshold	Value for the cycle threshold between 1 and 1000 milliseconds.

Command Default

None

Command History

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

The following example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
(Cisco Controller) > config band-select cycle-threshold 700
```

Related Commands

config band-select cycle-count

config band-select expire

config band-select client-rssi

config band-select expire

To set the entry expire for band select, use the **config band-select expire** command.

config band-select expire {**suppression** | **dual-band**} *seconds*

Syntax Description

suppression	Sets the suppression expire to the band select.
dual-band	Sets the dual band expire to the band select.
seconds	• Value for suppression between 10 to 200 seconds. • Value for a dual-band between 10 to 300 seconds.

Command Default

None

Command History

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

The following example shows how to set the suppression expire to 70 seconds:

```
(Cisco Controller) > config band-select expire suppression 70
```

Related Commands

config band-select cycle-threshold

config band-select client-rssi

config band-select cycle-count

config band-select client-rssi

To set the client received signal strength indicator (RSSI) threshold for band select, use the **config band-select client-rssi** command.

config band-select client-rssi *rssi*

Syntax Description

rssi	Minimum dBM of a client RSSI to respond to probe between 20 and 90.

Command Default

None

Command History

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

The following example shows how to set the RSSI threshold for band select to 70:

```
(Cisco Controller) > config band-select client-rssi 70
```

Related Commands

config band-select cycle-threshold

config band-select expire

config band-select cycle-count

config boot

To change a Cisco wireless LAN controller boot option, use the **config boot** command.

config boot {**primary** | **backup**}

Syntax Description

primary	Sets the primary image as active.
backup	Sets the backup image as active.

Command Default

The default boot option is **primary**.

Command History

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

Usage Guidelines

Each Cisco wireless LAN controller can boot off the primary, last-loaded operating system image (OS) or boot off the backup, earlier-loaded OS image.

The following example shows how to set the primary image as active so that the LAN controller can boot off the primary, last loaded image:

```
(Cisco Controller) > config boot primary
```

The following example shows how to set the backup image as active so that the LAN controller can boot off the backup, earlier loaded OS image:

```
(Cisco Controller) > config boot backup
```

Related Commands

show boot

config cdp

To configure the Cisco Discovery Protocol (CDP) on the controller, use the **config cdp** command.

config cdp {**enable** | **disable** | **advertise-v2** {**enable** | **disable**} | **timer***seconds* | **holdtime** *holdtime_interval*}

Syntax Description

enable	Enables CDP on the controller.
disable	Disables CDP on the controller.
advertise-v2	Configures CDP version 2 advertisements.
timer	Configures the interval at which CDP messages are to be generated.
seconds	Time interval at which CDP messages are to be generated. The range is from 5 to 254 seconds.
holdtime	Configures the amount of time to be advertised as the time-to-live value in generated CDP packets.
holdtime_interval	Maximum hold timer value. The range is from 10 to 255 seconds.

Command Default

The default value for CDP timer is 60 seconds.

The default value for CDP holdtime is 180 seconds.

Command History

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

The following example shows how to configure the CDP maximum hold timer to 150 seconds:

```
(Cisco Controller) > config cdp timer 150
```

Related Commands

config ap cdp

show cdp

show ap cdp

config certificate

To configure Secure Sockets Layer (SSL) certificates, use the **config certificate** command.

config certificate {**generate** {**webadmin** | **webauth**} | **compatibility** {**on** | **off**}}

Syntax Description

generate	Specifies authentication certificate generation settings.
webadmin	Generates a new web administration certificate.
webauth	Generates a new web authentication certificate.
compatibility	Specifies the compatibility mode for inter-Cisco wireless LAN controller IPsec settings.
on	Enables the compatibility mode.
off	Disables the compatibility mode.

Command Default

None

Command History

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

The following example shows how to generate a new web administration SSL certificate:

```
(Cisco Controller) > config certificate generate webadmin
Creating a certificate may take some time. Do you wish to continue? (y/n)
```

The following example shows how to configure the compatibility mode for inter-Cisco wireless LAN controller IPsec settings:

```
(Cisco Controller) > config certificate compatibility
```

Related Commands

config certificate lsc

show certificate compatibility

show certificate lsc

show certificate summary

show local-auth certificates

config certificate lsc

To configure Locally Significant Certificate (LSC) certificates, use the **config certificate lsc** command.

config certificate lsc {**enable** | **disable** | **ca-server** *http://url:port/path* | **ca-cert** {**add** | **delete**} | **subject-params** *country state city orgn dept email* | **other-params** *keysize*} | **ap-provision** {**auth-list** {**add** | **delete**} *ap_mac* | **revert-cert** *retries*}

Syntax Description

enable	Enables LSC certificates on the controller.
disable	Disables LSC certificates on the controller.
ca-server	Specifies the Certificate Authority (CA) server settings.
http://url:port/path	Domain name or IP address of the CA server.
ca-cert	Specifies CA certificate database settings.
add	Obtains a CA certificate from the CA server and adds it to the controller's certificate database.
delete	Deletes a CA certificate from the controller's certificate database.
subject-params	Specifies the device certificate settings.
country state city orgn dept email	Country, state, city, organization, department, and email of the certificate authority. **Note** The common name (CN) is generated automatically on the access point using the current MIC/SSC format *Cxxxx-MacAddr*, where *xxxx* is the product number.
other-params	Specifies the device certificate key size settings.
keysize	Value from 384 to 2048 (in bits); the default value is 2048.
ap-provision	Specifies the access point provision list settings.
auth-list	Specifies the provision list authorization settings.
ap_mac	MAC address of access point to be added or deleted from the provision list.
revert-cert	Specifies the number of times the access point attempts to join the controller using an LSC before reverting to the default certificate.

retries	Value from 0 to 255; the default value is 3.

Note If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate. If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Command Default

The default value of *keysize* is 2048 bits. The default value of *retries* is 3.

Command History

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

Usage Guidelines

You can configure only one CA server. To configure a different CA server, delete the configured CA server by using the **config certificate lsc ca-server delete** command, and then configure a different CA server.

If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in Step 8). If you do not configure an access point provision list, all access points with an MIC or SSC certificate that join the controller are LSC provisioned.

The following example shows how to enable the LSC settings:

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

This example shows how to enable the LSC settings for Certificate Authority (CA) server settings:

```
(Cisco Controller) >config certificate lsc ca-server http://10.0.0.1:8080/caserver
```

The following example shows how to add a CA certificate from the CA server and add it to the controller's certificate database:

```
(Cisco Controller) >config certificate lsc ca-cert add
```

The following example shows how to configure an LSC certificate with the keysize of 2048 bits:

```
(Cisco Controller) >config certificate lsc keysize 2048
```

config certificate ssc

To configure Self Signed Certificates (SSC) certificates, use the **config certificate ssc** command.

config certificate ssc hash validation {**enable** | **disable**}

Syntax Description

hash	Configures the SSC hash key.
validation	Configures hash validation of the SSC certificate.
enable	Enables hash validation of the SSC certificate.
disable	Disables hash validation of the SSC certificate.

Command Default

The SSC certificate is enabled by default..

Command History

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

Usage Guidelines

When you enable the SSC hash validation, an AP validates the SSC certificate of the virtual controller. When an AP validates the SSC certificate, it checks if the hash key of the virtual controller matches the hash key stored in its flash. If a match is found, the validation passes and the AP moves to the Run state. If a match is not found, the validation fails and the AP disconnects from the controller and restarts the discovery process. By default, hash validation is enabled. Hence, an AP must have the virtual controller hash key in its flash before associating with the virtual controller. If you disable hash validation of the SSC certificate, the AP bypasses the hash validation and directly moves to the Run state.

APs can associate with a physical controller, download the hash keys and then associate with a virtual controller. If the AP is associated to a physical controller and if hash validation is disabled, it joins any virtual controller without hash validation.

The following example shows how to enable hash validation of the SSC certificate:

```
(Cisco Controller) > config certificate ssc hash validation enable
```

Related Commands

show certificate ssc

show mobility group member

config mobility group member hash

config certificate

show certificate compatibility

show certificate lsc

show certificate summary

show local-auth certificates

config certificate use-device-certificate webadmin

To use a device certificate for web administration, use the **config certificate use-device-certificate webadmin** command.

config certificate use-device-certificate webadmin

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to use a device certificate for web administration:

```
(Cisco Controller) > config certificate use-device-certificate webadmin
Use device certificate for web administration. Do you wish to continue? (y/n) y
Using device certificate for web administration.
Save configuration and restart controller to use new certificate.
```

Related Commands

config certificate

show certificate compatibility

show certificate lsc

show certificate ssc

show certificate summary

show local-auth certificates

config coredump

To enable or disable the controller to generate a core dump file following a crash, use the **config cordump** command.

config coredump {**enable** | **disable**}

Syntax Description

enable	Enables the controller to generate a core dump file.
disable	Disables the controller to generate a core dump file.

Command Default

None

Command History

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

The following example shows how to enable the controller to generate a core dump file following a crash:

```
(Cisco Controller) > config coredump enable
```

Related Commands

config coredump ftp

config coredump username

show coredump summary

config coredump ftp

To automatically upload a controller core dump file to an FTP server after experiencing a crash, use the **config coredump ftp** command.

config coredump ftp *server_ip_address filename*

Syntax Description

server_ip_address	IP address of the FTP server to which the controller sends its core dump file.
filename	Name given to the controller core dump file.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

The controller must be able to reach the FTP server to use this command.

The following example shows how to configure the controller to upload a core dump file named *core_dump_controller* to an FTP server at network address *192.168.0.13*:

```
(Cisco Controller) > config coredump ftp 192.168.0.13 core_dump_controller
```

Related Commands

config coredump

config coredump username

show coredump summary

config coredump username

To specify the FTP server username and password when uploading a controller core dump file after experiencing a crash, use the **config coredump username** command.

config coredump username *ftp_username* **password** *ftp_password*

Syntax Description

ftp_username	FTP server login username.
ftp_password	FTP server login password.

Command Default

None

Command History

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

Usage Guidelines

The controller must be able to reach the FTP server to use this command.

The following example shows how to specify a FTP server username of *admin* and password *adminpassword* for the core dump file upload:

```
(Cisco Controller) > config coredump username admin password adminpassword
```

Related Commands

config coredump ftp

config coredump

show coredump summary

config custom-web ext-webauth-mode

To configure external URL web-based client authorization for the custom-web authentication page, use the **config custom-web ext-webauth-mode** command.

config custom-web ext-webauth-mode {**enable** | **disable**}

Syntax Description

enable	Enables the external URL web-based client authorization.
disable	Disables the external URL we-based client authentication.

Command Default

None

Command History

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

The following example shows how to enable the external URL web-based client authorization:

```
(Cisco Controller) > config custom-web ext-webauth-mode enable
```

Related Commands

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-url show custom-web

config custom-web ext-webauth-url

To configure the complete external web authentication URL for the custom-web authentication page, use the **config custom-web ext-webauth-url** command.

config custom-web ext-webauth-url *URL*

Syntax Description

URL	URL used for web-based client authorization.

Command Default

None

Command History

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

The following example shows how to configure the complete external web authentication URL http://www.AuthorizationURL.com/ for the web-based client authorization:

```
(Cisco Controller) > config custom-web ext-webauth-url http://www.AuthorizationURL.com/
```

Related Commands

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode show custom-web

config custom-web ext-webserver

To configure an external web server, use the **config custom-web ext-webserver** command.

config custom-web ext-webserver {**add** *index IP_address* | **delete** *index*}

Syntax Description

add	Adds an external web server.
index	Index of the external web server in the list of external web server. The index must be a number between 1 and 20.
IP_address	IP address of the external web server.
delete	Deletes an external web server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

The following example shows how to add the index of the external web server 2 to the IP address of the external web server 192.23.32.19:

```
(Cisco Controller) > config custom-web ext-webserver add 2 192.23.32.19
```

Related Commands

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web logout-popup

To enable or disable the custom web authentication logout popup, use the **config custom-web logout-popup** command.

config custom-web logout-popup {**enable** | **disable**}

Syntax Description

enable	Enables the custom web authentication logout popup. This page appears after a successful login or a redirect of the custom web authentication page.
disable	Disables the custom web authentication logout popup.

Command Default

None

Command History

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

The following example shows how to disable the custom web authentication logout popup:

```
(Cisco Controller) > config custom-web logout-popup disable
```

Related Commands

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-url show custom-web

config custom-web redirectUrl

To configure the redirect URL for the custom-web authentication page, use the **config custom-web redirectUrl** command.

config custom-web redirectUrl *URL*

Syntax Description

URL	URL that is redirected to the specified address.

Command Default

None

Command History

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

The following example shows how to configure the URL that is redirected to abc.com:

```
(Cisco Controller) > config custom-web redirectUrl abc.com
```

Related Commands

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web webauth-type

To configure the type of web authentication, use the **config custom-web webauth-type** command.

config custom-web webauth-type {**internal** | **customized** | **external**}

Syntax Description

internal	Configures the web authentication type to internal.
customized	Configures the web authentication type to customized.
external	Configures the web authentication type to external.

Command Default

The default web authentication type is **internal**.

Command History

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

The following example shows how to configure the type of the web authentication type to internal:

```
(Cisco Controller) > config custom-web webauth-type internal
```

Related Commands

config custom-web redirectUrl

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web weblogo

To configure the web authentication logo for the custom-web authentication page, use the **config custom-web weblogo** command.

config custom-web weblogo {**enable** | **disable**}

Syntax Description

enable	Enables the web authentication logo settings.
disable	Enable or disable the web authentication logo settings.

Command Default

None

Command History

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

The following example shows how to enable the web authentication logo:

```
(Cisco Controller) > config custom-web weblogo enable
```

Related Commands

config custom-web redirectUrl

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web webmessage

To configure the custom web authentication message text for the custom-web authentication page, use the **config custom-web webmessage** command.

config custom-web webmessage *message*

Syntax Description

message	Message text for web authentication.

Command Default

None

Command History

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

The following example shows how to configure the message text Thisistheplace for webauthentication:

```
(Cisco Controller) > config custom-web webmessage Thisistheplace
```

Related Commands

config custom-web redirectUrl

config custom-web weblogo

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web webtitle

To configure the web authentication title text for the custom-web authentication page, use the **config custom-web webtitle** command.

config custom-web webtitle *title*

Syntax Description

title	Custom title text for web authentication.

Command Default

None

Command History

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

The following example shows how to set the custom title text Helpdesk for web authentication:

```
(Cisco Controller) > config custom-web webtitle Helpdesk
```

Related Commands

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config dhcp

To configure the internal DHCP, use the **config dhcp** command.

config dhcp {**address-pool** *scope start end* | **create-scope** *scope* | **default-router** *scope router_1* [*router_2*] [*router_3*] | **delete-scope** *scope* | **disable** *scope* | **dns-servers** *scope dns1* [*dns2*] [*dns3*] | **domain** *scope domain* | **enable** *scope* | **lease** *scope lease_duration* | **netbios-name-server** *scope wins1* [*wins2*] [*wins3*] | **network***scope network netmask*}

config dhcpopt-82 remote-id {*ap_mac* | *ap_mac***:***ssid* | *ap-ethmac* | *apname:ssid* | *ap-group-name* | *flex-group-name* | *ap-location* | *apmac-vlan_id* | *apname-vlan_id* | *ap-ethmac-ssid* }

Syntax Description

address-pool *scope start end*	Configures an address range to allocate. You must specify the scope name and the first and last addresses of the address range.
create-scope *name*	Creates a new DHCP scope. You must specify the scope name.
default-router *scope router_1* [*router_2*] [*router_3*]	Configures the default routers for the specified scope and specify the IP address of a router. Optionally, you can specify the IP addresses of secondary and tertiary routers.
delete-scope *scope*	Deletes the specified DHCP scope.
disable *scope*	Disables the specified DHCP scope.
dns-servers *scope dns1* [*dns2*] [*dns3*]	Configures the name servers for the given scope. You must also specify at least one name server. Optionally, you can specify secondary and tertiary name servers.
domain *scope domain*	Configures the DNS domain name. You must specify the scope and domain names.
enable *scope*	Enables the specified dhcp scope.
lease *scope lease_duration*	Configures the lease duration (in seconds) for the specified scope.
netbios-name-server *scope wins1* [*wins2*] [*wins3*]	Configures the netbios name servers. You must specify the scope name and the IP address of a name server. Optionally, you can specify the IP addresses of secondary and tertiary name servers.
network *scope network netmask*	Configures the network and netmask. You must specify the scope name, the network address, and the network mask.

opt-82 remote-id	Configures the DHCP option 82 remote ID field format. DHCP option 82 provides additional security when DHCP is used to allocate network addresses. The controller acts as a DHCP relay agent to prevent DHCP client requests from untrusted sources. The controller adds option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.
ap_mac	MAC address of the access point to the DHCP option 82 payload.
*ap_mac***:***ssid*	MAC address and SSID of the access point to the DHCP option 82 payload.
ap-ethmac	Remote ID format as AP Ethernet MAC address.
apname:ssid	Remote ID format as AP name:SSID.
ap-group-name	Remote ID format as AP group name.
flex-group-name	Remote ID format as FlexConnect group name .
ap-location	Remote ID format as AP location.
apmac-vlan_id	Remote ID format as AP radio MAC address:VLAN_ID.
apname-vlan_id	Remote ID format as AP Name:VLAN_ID.
ap-ethmac-ssid	Remote ID format as AP Ethernet MAC:SSID address.

Command Default

The default value for ap-group-name is default-group, and for ap-location, the default value is default location.

If ap-group-name and flex-group-name are null, the system MAC is sent as the remote ID field.

Command History

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

Usage Guidelines

Use the **show dhcp** command to display the internal DHCP configuration.

The following example shows how to configure the DHCP lease for the scope 003:

```
(Cisco Controller) >config dhcp lease 003
```

config dhcp proxy

To specify the level at which DHCP packets are modified, use the **config dhcp proxy** command.

config dhcp proxy {**enable** | **disable** {**bootp-broadcast** [**enable** | **disable**]}

Syntax Description

enable	Allows the controller to modify the DHCP packets without a limit.
disable	Reduces the DHCP packet modification to the level of a relay.
bootp-broadcast	Configures DHCP BootP broadcast option.

Command Default

DHCP is enabled.

Command History

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

Usage Guidelines

Use the **show dhcp proxy** command to display the status of DHCP proxy handling.

To enable third-party WGB support, you must enable the passive-client feature on the wirless LAN by entering the **config wlan passive-client enable** command.

The following example shows how to disable the DHCP packet modification:

```
(Cisco Controller) >config dhcp proxy disable
```

The following example shows how to enable the DHCP BootP broadcast option:

```
(Cisco Controller) >config dhcp proxy disable bootp-broadcast enable
```

config dhcp timeout

To configure a DHCP timeout value, use the **config dhcp timeout** command. If you have configured a WLAN to be in DHCP required state, this timer controls how long the WLC will wait for a client to get a DHCP lease through DHCP.

config dhcp timeout *timeout-value*

Syntax Description

timeout-value	Timeout value in the range of 5 to 120 seconds.

Command Default

The default timeout value is 120 seconds.

Command History

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

The following example shows how to set the DHCP timeout to 10 seconds:

```
(Cisco Controller) >config dhcp timeout 10
```

config flexconnect avc profile

To configure a Flexconnect Application Visibility and Control (AVC) profile, use the **config flexconnect avc profile** command.

config flexconnect avc profile *profilename* {**create | delete**} | **apply** | **rule** {**addapplication** *app-name* {**drop** | {**mark** *dscp-value*}}} | {**remove application** *app-name*}

Syntax Description

proflie-name	Name of the AVC profile. The range is from 0 to 32 alphanumeric characters.
create	Creates an AVC profile.
delete	Deletes an AVC profile.
apply	Applies an AVC profile.
rule	Configures a Rule for an AVC profile.
add application	Adds a rule for an AVC profile.
app-name	Name of the application. The range is from 0 to 32 alphanumeric characters.
drop	Adds a rule to drop packets.
mark	Adds a rule to mark packets with specific differentiated services code point (DSCP).
dscp-value	DSCP value for marking packets. The range is from 0 to 63.
remove application	Removes a rule for an AVC profile.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to create a FlexConnect profile:

```
(Cisco Controller) >config flexconnect avc profile profile1 create
```

config flow

To configure a NetFlow Monitor and Exporter, use the **config flow** command.

config flow {**add** | **delete**} **monitor** *monitor_name* {**exporter** *exporter_name* | **record**{*ipv4_client_app_flow_record* | *ipv4_client_src_dst_flow_record*}

Syntax Description

add	Associates either a NetFlow monitor with an exporter, or a NetFlow record with a NetFlow monitor.
delete	Dissociates either a NetFlow monitor from an exporter, or a NetFlow record from a NetFlow monitor.
monitor	Configures a NetFlow monitor.
monitor_name	Name of the NetFlow monitor. The monitor name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces in a monitor name.
exporter	Configures a NetFlow exporter.
exporter_name	Name of the NetFlow exporter. The exporter name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces in an exporter name.
record	Associates a NetFlow record to the NetFlow monitor.
ipv4_client_app_flow_record	Existing record template for better performance.

Command Default

None

Command History

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

Usage Guidelines

An exporter is a network entity that exports the template with IP traffic information. The Cisco WLC acts as an exporter. A NetFlow record in the Cisco WLC contains the information about the traffic in a given flow, such as client MAC address, client source IP address, WLAN ID, incoming and outgoing bytes of data, incoming and outgoing packets, and incoming and outgoing Differentiated Services Code Point (DSCP).

The following example shows how to configure a NetFlow monitor and exporter:

```
(Cisco Controller) > config flow add monitor monitor1 exporter exporter1
```

config guest-lan

To create, delete, enable or disable a wireless LAN, use the **config guest-lan** command.

config guest-lan {**create** | **delete**} *guest_lan_id interface_name* | {**enable** | **disable**} *guest_lan_id*

Syntax Description

create	Creates a wired LAN settings.
delete	Deletes a wired LAN settings:
guest_lan_id	LAN identifier between 1 and 5 (inclusive).
interface_name	Interface name up to 32 alphanumeric characters.
enable	Enables a wireless LAN.
disable	Disables a wireless LAN.

Command Default

None

Command History

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

The following example shows how to enable a wireless LAN with the LAN ID 16:

```
(Cisco Controller) > config guest-lan enable 16
```

Related Commands

show wlan

config guest-lan custom-web ext-webauth-url

To redirect guest users to an external server before accessing the web login page, use the **config guest-lan custom-web ext-webauth-url** command.

config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

Syntax Description

ext_web_url	URL for the external server.
guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).

Command Default

None

Command History

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

The following example shows how to enable a wireless LAN with the LAN ID 16:

```
(Cisco Controller) > config guest-lan custom-web ext-webauth-url
http://www.AuthorizationURL.com/ 1
```

Related Commands

config guest-lan

config guest-lan create

config guest-lan custom-web login_page

config guest-lan custom-web global disable

To use a guest-LAN specific custom web configuration rather than a global custom web configuration, use the **config guest-lan custom-web global disable** command.

config guest-lan custom-web global disable *guest_lan_id*

Syntax Description

guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).

Command Default

None

Command History

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

Usage Guidelines

If you enter the **config guest-lan custom-web global enable** *guest_lan_id* command, the custom web authentication configuration at the global level is used.

The following example shows how to disable the global web configuration for guest LAN ID 1:

```
(Cisco Controller) > config guest-lan custom-web global disable 1
```

Related Commands

config guest-lan

config guest-lan create

config guest-lan custom-web ext-webauth-url

config guest-lan custom-web login_page

config guest-lan custom-web webauth-type

config guest-lan custom-web login_page

To enable wired guest users to log into a customized web login page, use the **config guest-lan custom-web login_page** command.

config guest-lan custom-web login_page *page_name guest_lan_id*

Syntax Description

page_name	Name of the customized web login page.
guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).

Command Default

None

Command History

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

The following example shows how to customize a web login page custompage1 for guest LAN ID 1:

```
(Cisco Controller) > config guest-lan custom-web login_page custompage1 1
```

Related Commands

config guest-lan

config guest-lan create

config guest-lan custom-web ext-webauth-url

config guest-lan custom-web webauth-type

To define the web login page for wired guest users, use the **config guest-lan custom-web webauth-type** command.

config guest-lan custom-web webauth-type {**internal** | **customized** | **external**} *guest_lan_id*

Syntax Description

internal	Displays the default web login page for the controller. This is the default value.
customized	Displays the custom web login page that was previously configured.
external	Redirects users to the URL that was previously configured.
guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).

Command Default

The default web login page for the controller is internal.

Command History

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

The following example shows how to configure the guest LAN with the webauth-type as internal for guest LAN ID 1:

```
(Cisco Controller) > config guest-lan custom-web webauth-type internal 1
```

Related Commands

config guest-lan

config guest-lan create

config guest-lan custom-web ext-webauth-url

config guest-lan ingress-interface

To configure the wired guest VLAN's ingress interface that provides a path between the wired guest client and the controller through the Layer 2 access switch, use the **config guest-lan ingress-interface** command.

config guest-lan ingress-interface *guest_lan_id interface_name*

Syntax Description

guest_lan_id	Guest LAN identifier from 1 to 5 (inclusive).
interface_name	Interface name.

Command Default

None

Command History

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

The following example shows how to provide a path between the wired guest client and the controller with guest LAN ID 1 and the interface name guest01:

```
(Cisco Controller) > config guest-lan ingress-interface 1 guest01
```

Related Commands

config interface guest-lan

config guest-lan create

config guest-lan interface

To configure an egress interface to transmit wired guest traffic out of the controller, use the **config guest-lan interface** command.

config guest-lan interface *guest_lan_id interface_name*

Syntax Description

guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).
interface_name	Interface name.

Command Default

None

Command History

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

The following example shows how to configure an egress interface to transmit guest traffic out of the controller for guest LAN ID 1 and interface name guest01:

```
(Cisco Controller) > config guest-lan interface 1 guest01
```

Related Commands

config ingress-interface guest-lan

config guest-lan create

config guest-lan mobility anchor

To add or delete mobility anchor, use the **config guest-lan mobility anchor** command.

config guest-lan mobility anchor {**add** | **delete**} *Guest LAN Id IP addr*

Syntax Description

add	Adds a mobility anchor to a WLAN.
delete	Deletes a mobility anchor from a WLAN.
Guest LAN Id	Guest LAN identifier between 1 and 5.
IP addr	Member switch IPv4 or IPv6 address to anchor WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to delete a mobility anchor for WAN ID 4 and the anchor IP *192.168.0.14*:

```
(Cisco Controller) > config guest-lan mobility anchor delete 4 192.168.0.14
```

config guest-lan nac

To enable or disable Network Admission Control (NAC) out-of-band support for a guest LAN, use the **config guest-lan nac** command:

config guest-lan nac {**enable** | **disable**} *guest_lan_id*

Syntax Description

enable	Enables the NAC out-of-band support.
disable	Disables the NAC out-of-band support.
guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).

Command Default

None

Command History

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

The following example shows how to enable the NAC out-of-band support for guest LAN ID 3:

```
(Cisco Controller) > config guest-lan nac enable 3
```

Related Commands

show nac statistics

show nac summary

config wlan nac

debug nac

config guest-lan security

To configure the security policy for the wired guest LAN, use the **config guest-lan security** command.

config guest-lan security {**web-auth** {**enable** | **disable** | **acl** | **server-precedence**} *guest_lan_id* | **web-passthrough** {**acl** | **email-input** | **disable** | **enable**} *guest_lan_id*}

Syntax Description

web-auth	Specifies web authentication.
enable	Enables the web authentication settings.
disable	Disables the web authentication settings.
acl	Configures an access control list.
server-precedence	Configures the authentication server precedence order for web authentication users.
guest_lan_id	LAN identifier between 1 and 5 (inclusive).
web-passthrough	Specifies the web captive portal with no authentication required.
email-input	Configures the web captive portal using an e-mail address.

Command Default

The default security policy for the wired guest LAN is web authentication.

Command History

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

The following example shows how to configure the security web authentication policy for guest LAN ID 1:

```
(Cisco Controller) > config guest-lan security web-auth enable 1
```

Related Commands

config ingress-interface guest-lan

config guest-lan create

config interface guest-lan

config license agent

To configure the license agent on the Cisco 5500 Series Controller, use the **config license agent** command.

config license agent {**default** {**disable** | **authenticate** [**none**]} } {**listener http** {**disable** | {**plaintext** | **encrypt**} **url authenticate** [**acl** *acl_name*] {**max-message** *size* [**none**]} } {**max-session** *sessions*} {**notify** {**disable** | *url*} *username password*}

Syntax Description

default	Specifies the default license agent.
disable	Disables the feature.
authenticate	Enables authentication.
none	(Optional) Disables authentication.
listener http	Configures the license agent to receive license requests from the Cisco License Manager (CLM).
plaintext	Disables encryption (HTTP).
encrypt	Enables encryption (HTTPS).
url	URL where the license agent receives the requests.
acl	(Optional) Specifies the access control list.
acl_name	Specifies the access control list for license requests.
max-message	Specifies the maximum message size for license requests.
size	Maximum message size for license request is from 0 to 65535.
max-session	Specifies the maximum number of sessions allowed.
sessions	Maximum number of sessions allowed for the license agent is from 1 to 25.
notify	Configures the license agent to send license notifications to the CLM.
username	Username used in license agent notification.
password	Password used in license agent notification.

Command Default

The license agent is **disabled** by default.

The listener is **disabled** by default.

Notify is **disabled** by default.

The default maximum number of sessions is 9.

The default maximum message size is 0.

Command History

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

Usage Guidelines

If your network contains various Cisco licensed devices, you might consider using the CLM to manage all of the licenses using a single application. CLM is a secure client/server application that manages Cisco software licenses network wide.

The license agent is an interface module that runs on the controller and mediates between CLM and the controller's licensing infrastructure. CLM can communicate with the controller using various channels, such as HTTP, Telnet, and so on. If you want to use HTTP as the communication method, you must enable the license agent on the controller.

The license agent receives requests from the CLM and translates them into license commands. It also sends notifications to the CLM. It uses XML messages over HTTP or HTTPS to receive the requests and send the notifications. For example, if the CLM sends a **license clear** command, the agent notifies the CLM after the license expires.

Note You can download the CLM software and access user documentation at this URL: http://www.cisco.com/c/en/us/products/cloud-systems-management/license-manager/index.html

The following example shows how to authenticate the default license agent settings:

```
(Cisco Controller) > config license agent default authenticate
```

The following example shows how to configure the license agent with the number of maximum sessions allowed as 5:

```
(Cisco Controller) > config license agent max-session 5
```

Related Commands

license install

show license agent

clear license agent

config license boot

To specify the license level to be used on the next reboot of the Cisco 5500 Series Controller, use the **config license boot** command.

config license boot {**base** | **wplus** | **auto**}

Syntax Description

base	Specifies the base boot level.
wplus	Specifies the wplus boot level.
auto	Specifies the auto boot level.

Command Default

None

Command History

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

Usage Guidelines

If you enter **auto**, the licensing software automatically chooses the license level to use on the next reboot. It generally chooses permanent licenses over evaluation licenses and wplus licenses over base licenses.

Note If you are considering upgrading from a base license to a wplus license, you can try an evaluation wplus license before upgrading to a permanent wplus license. To activate the evaluation license, you need to set the image level to wplus in order for the controller to use the wplus evaluation license instead of the base permanent license.

Note To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

The following example shows how to set the license boot settings to wplus:

```
(Cisco Controller) > config license boot wplus
```

Related Commands

license install

show license in-use

license modify priority

config load-balancing

To globally configure aggressive load balancing on the controller, use the **config load-balancing** command.

config load-balancing {**window** *client_count* | **status** {**enable** | **disable**} | **denial** *denial_count*}

config load-balancing uplink-threshold *traffic_threshold*

Syntax Description

window	Specifies the aggressive load balancing client window.
client_count	Aggressive load balancing client window with the number of clients from 1 to 20.
status	Sets the load balancing status.
enable	Enables load balancing feature.
disable	Disables load balancing feature.
denial	Specifies the number of association denials during load balancing.
denial_count	Maximum number of association denials during load balancing. from 0 to 10.
uplink-threshold	Specifies the threshold traffic for an access point to deny new associations.
traffic_threshold	Threshold traffic for an access point to deny new associations. This value is a percentage of the WAN utilization measured over a 90 second interval. For example, the default threshold value of 50 triggers the load balancing upon detecting an utilization of 50% or more on an access point WAN interface.

Command Default

By default, the aggressive load balancing is disabled.

Command History

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

Usage Guidelines

Load-balancing-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

When you use Cisco 7921 and 7920 Wireless IP Phones with controllers, make sure that aggressive load balancing is disabled on the voice WLANs for each controller. Otherwise, the initial roam attempt by the phone might fail, causing a disruption in the audio path.

Clients can only be load balanced across access points joined to the same controller. The WAN utilization is calculated as a percentage using the following formula: (Transmitted Data Rate (per second) + Received Data Rate (per second))/(1000Mbps TX + 1000Mbps RX) * 100

The following example shows how to enable the aggressive load-balancing settings:

```
(Cisco Controller) > config load-balancing aggressive enable
```

Related Commands

show load-balancing

config wlan load-balance

config location

To configure a location-based system, use the **config location** command.

config location {**algorithm** {**simple** | **rssi-average**} | {**rssi-half-life** | **expiry**} [**client** | **calibrating-client** | **tags** | **rogue-aps**] *seconds* | **notify-threshold** [**client** | **tags** | **rogue-aps**] *threshold* | **interface-mapping** {**add** | **delete**} *location wlan_id interface_name* | **plm** {**client** {**enable** | **disable**} *burst_interval* | **calibrating** {**enable** | **disable**} {**uniband** | **multiband**}}}

Syntax Description

algorithm	**Note** We recommend that you do not use or modify the **config location algorithm** command. It is set to optimal default values. Configures the algorithm used to average RSSI and SNR values.
simple	Specifies a faster algorithm that requires low CPU overhead but provides less accuracy.
rssi-average	Specifies a more accurate algorithm but requires more CPU overhead.
rssi-half-life	**Note** We recommend that you do not use or modify the **config location rssi-half-life** command. It is set to optimal default values. Configures the half-life when averaging two RSSI readings.
expiry	**Note** We recommend that you do not use or modify the **config location expiry** command. It is set to optimal default values. Configures the timeout for RSSI values.
client	(Optional) Specifies the parameter applies to client devices.
calibrating-client	(Optional) Specifies the parameter is used for calibrating client devices.
tags	(Optional) Specifies the parameter applies to radio frequency identification (RFID) tags.
rogue-aps	(Optional) Specifies the parameter applies to rogue access points.

seconds	Time value (0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, 300 seconds).
notify-threshold	**Note** We recommend that you do not use or modify the **config location notify-threshold** command. It is set to optimal default values. Specifies the NMSP notification threshold for RSSI measurements.
threshold	Threshold parameter. The range is 0 to 10 dB, and the default value is 0 dB.
interface-mapping	Adds or deletes a new location, wireless LAN, or interface mapping element.
wlan_id	WLAN identification name.
interface_name	Name of interface to which mapping element applies.
plm	Specifies the path loss measurement (S60) request for normal clients or calibrating clients.
client	Specifies normal, noncalibrating clients.
burst_interval	Burst interval. The range is from 1 to 3600 seconds, and the default value is 60 seconds.
calibrating	Specifies calibrating clients.
uniband	Specifies the associated 802.11a or 802.11b/g radio (uniband).
multiband	Specifies the associated 802.11a/b/g radio (multiband).

Command Default

See the "Syntax Description" section for default values of individual arguments and keywords.

Command History

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

The following example shows how to specify the simple algorithm for averaging RSSI and SNR values on a location-based controller:

```
(Cisco Controller) > config location algorithm simple
```

Related Commands

config location info rogue

clear location rfid

clear location statistics rfid

show location

show location statistics rfid

config location info rogue

To configure info-notification for rogue service, use the **config location info rogue** command.

config location info rogue {**basic** | **extended**}

Syntax Description

basic	Configures basic rogue parameters such as mode, class, containmentlevel, numclients, firsttime, lasttime, ssid, and so on, for rogue info-notification service. **Note** Configure the basic parameters if the version of Cisco MSE is older than the version of the Cisco WLC.
extended	Configures extended rogue parameters, which is basic parameters plus security type, detecting LRAD type, and so on, for rogue info-notification service.

Command History

Release	Modification
8.0	This command was introduced.

config logging buffered

To set the severity level for logging messages to the controller buffer, use the **config logging buffered** command.

config logging buffered `security_level`

Syntax Description

security_level	Security level. Choose one of the following: • 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

Command Default

None

Command History

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

The following example shows how to set the controller buffer severity level for logging messages to 4:

```
(Cisco Controller) > config logging buffered 4
```

Related Commands

config logging syslog facility

config logging syslog level

show logging

config logging console

To set the severity level for logging messages to the controller console, use the **config logging console** command.

config logging console *security_level*

Syntax Description

security_level	Severity level. Choose one of the following: • 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

Command Default

None

Command History

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

The following example shows how to set the controller console severity level for logging messages to 3:

```
(Cisco Controller) > config logging console 3
```

Related Commands

config logging syslog facility

config logging syslog level

show logging

config logging debug

To save debug messages to the controller buffer, the controller console, or a syslog server, use the **config logging debug** command.

config logging debug {**buffered** | **console** | **syslog**} {**enable** | **disable**}

Syntax Description

buffered	Saves debug messages to the controller buffer.
console	Saves debug messages to the controller console.
syslog	Saves debug messages to the syslog server.
enable	Enables logging of debug messages.
disable	Disables logging of debug messages.

Command Default

The **console** command is enabled and the **buffered** and **syslog** commands are disabled by default.

Command History

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

The following example shows how to save the debug messages to the controller console:

```
(Cisco Controller) > config logging debug console enable
```

Related Commands

show logging

config logging fileinfo

To cause the controller to include information about the source file in the message logs or to prevent the controller from displaying this information, use the **config logging fileinfo** command.

config logging fileinfo {**enable** | **disable**}

Syntax Description

enable	Includes information about the source file in the message logs.
disable	Prevents the controller from displaying information about the source file in the message logs.

Command Default

None

Command History

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

The following example shows how to enable the controller to include information about the source file in the message logs:

```
(Cisco Controller) > config logging fileinfo enable
```

Related Commands

show logging

config logging procinfo

To cause the controller to include process information in the message logs or to prevent the controller from displaying this information, use the **config logging procinfo** command.

config logging procinfo {**enable** | **disable**}

Syntax Description

enable	Includes process information in the message logs.
disable	Prevents the controller from displaying process information in the message logs.

Command Default

None

Command History

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

The following example shows how to enable the controller to include the process information in the message logs:

```
(Cisco Controller) > config logging procinfo enable
```

Related Commands

show logging

config logging traceinfo

To cause the controller to include traceback information in the message logs or to prevent the controller from displaying this information, use the **config logging traceinfo** command.

config logging traceinfo {**enable** | **disable**}

Syntax Description

enable	Includes traceback information in the message logs.
disable	Prevents the controller from displaying traceback information in the message logs.

Command Default

None

Command History

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

The following example shows how to disable the controller to include the traceback information in the message logs:

```
(Cisco Controller) > config logging traceinfo disable
```

Related Commands

show logging

config logging syslog host

To configure a remote host for sending syslog messages, use the **config logging syslog host** command.

config logging syslog host *ip_addr*

Syntax Description

ip_addr	IP address for the remote host.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

- To configure a remote host for sending syslog messages, use the **config logging syslog host** *ip_addr* command.
- To remove a remote host that was configured for sending syslog messages, use the **config logging syslog host** *ip_addr* **delete** command.
- To display the configured syslog servers on the controller, use the **show logging** command.

The following example shows how to configure two remote hosts 10.92.125.52 and 2001:9:6:40::623 for sending the syslog messages and displaying the configured syslog servers on the controller:

```
(Cisco Controller) > config logging syslog host 10.92.125.52
System logs will be sent to 10.92.125.52 from now on

(Cisco Controller) > config logging syslog host 2001:9:6:40::623
System logs will be sent to 2001:9:6:40::623 from now on

(Cisco Controller) > show logging
Logging to buffer :
- Logging of system messages to buffer :
 - Logging filter level..................... errors
 - Number of system messages logged..... 1316
 - Number of system messages dropped..... 6892
- Logging of debug messages to buffer ..... Disabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Cache of logging  ..... Disabled
- Cache of logging time(mins) ..... 10080
- Number of over cache time log dropped  ..... 0
Logging to console :
- Logging of system messages to console :
 - Logging filter level..... disabled
 - Number of system messages logged..... 0
 - Number of system messages dropped..... 8243
- Logging of debug messages to console ..... Enabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
Logging to syslog :
```

```
- Syslog facility.............................. local0
- Logging of system messages to console :
 - Logging filter level........................ disabled
 - Number of system messages logged............. 0
 - Number of system messages dropped............ 8208
- Logging of debug messages to console ......... Enabled
 - Number of debug messages logged.............. 0
 - Number of debug messages dropped............. 0
- Logging of system messages to syslog :
 - Logging filter level........................ errors
 - Number of system messages logged............. 1316
 - Number of system messages dropped............ 6892
- Logging of debug messages to syslog ........... Disabled
 - Number of debug messages logged.............. 0
 - Number of debug messages dropped............. 0
- Number of remote syslog hosts................. 2
- syslog over tls............................... Disabled
  - Host 0..................................... 10.92.125.52
  - Host 1..................................... 2001:9:6:40::623
  - Host 2.....................................
Logging of RFC 5424............................ Disabled
Logging of Debug messages to file :
- Logging of Debug messages to file............. Disabled
- Number of debug messages logged............... 0
- Number of debug messages dropped.............. 0
Logging of traceback........................... Enabled
```

The following example shows how to remove two remote hosts 10.92.125.52 and 2001:9:6:40::623 that were configured for sending syslog messages and displaying that the configured syslog servers were removed from the controller:

```
(Cisco Controller) > config logging syslog host 10.92.125.52 delete
System logs will not be sent to 10.92.125.52 anymore

(Cisco Controller) > config logging syslog host 2001:9:6:40::623 delete
System logs will not be sent to 2001:9:6:40::623 anymore

(Cisco Controller) > show logging

Logging to buffer :
- Logging of system messages to buffer :
 - Logging filter level........................ errors
 - Number of system messages logged............. 1316
 - Number of system messages dropped............ 6895
- Logging of debug messages to buffer ........... Disabled
 - Number of debug messages logged.............. 0
 - Number of debug messages dropped............. 0
- Cache of logging  ............................ Disabled
- Cache of logging time(mins) ................... 10080
- Number of over cache time log dropped  ........ 0
Logging to console :
- Logging of system messages to console :
 - Logging filter level........................ disabled
 - Number of system messages logged............. 0
 - Number of system messages dropped............ 8211
- Logging of debug messages to console ......... Enabled
 - Number of debug messages logged.............. 0
 - Number of debug messages dropped............. 0
Logging to syslog :
- Syslog facility.............................. local0
- Logging of system messages to syslog :
 - Logging filter level........................ errors
 - Number of system messages logged............. 1316
```

```
 - Number of system messages dropped.............. 6895
- Logging of debug messages to syslog ........... Disabled
 - Number of debug messages logged................ 0
 - Number of debug messages dropped............... 0
- Number of remote syslog hosts.................. 0
- syslog over tls................................ Disabled
  - Host 0.......................................
  - Host 1.......................................
  - Host 2.......................................
Logging of RFC 5424.............................. Disabled
Logging of Debug messages to file :
- Logging of Debug messages to file.............. Disabled
- Number of debug messages logged................ 0
- Number of debug messages dropped............... 0
Logging of traceback............................. Enabled
- Traceback logging level........................ errors
Logging of source file informational............. Enabled
Timestamping of messages.........................
- Timestamping of system messages................ Enabled
 - Timestamp format.............................. Date and Time
```

Related Topics

show logging, on page 421

config logging syslog facility

To set the facility for outgoing syslog messages to the remote host, use the **config logging syslog facility** command.

config logging syslog facility *facility_code*

Syntax Description

facility_code	Facility code. Choose one of the following: • authorization—Authorization system. Facility level—4. • auth-private—Authorization system (private). Facility level—10. • cron—Cron/at facility. Facility level—9. • daemon—System daemons. Facility level—3. • ftp—FTP daemon. Facility level—11. • kern—Kernel. Facility level—0. • local0—Local use. Facility level—16. • local1—Local use. Facility level—17. • local2—Local use. Facility level—18. • local3—Local use. Facility level—19. • local4—Local use. Facility level—20. • local5—Local use. Facility level—21. • local6—Local use. Facility level—22. • local7—Local use. Facility level—23. • lpr—Line printer system. Facility level—6. • mail—Mail system. Facility level—2. • news—USENET news. Facility level—7. • sys12—System use. Facility level—12. • sys13—System use. Facility level—13. • sys14—System use. Facility level—14. • sys15—System use. Facility level—15. • syslog—The syslog itself. Facility level—5. • user—User process. Facility level—1. • uucp—UNIX-to-UNIX copy system. Facility level—8.

Command Default

None

Command History

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

The following example shows how to set the facility for outgoing syslog messages to authorization:

```
(Cisco Controller) > config logging syslog facility authorization
```

Related Commands

config logging syslog host

config logging syslog level

show logging

config logging syslog facility client

To configure the syslog facility to AP, use the **config logging syslog facility client** { **assocfail Dot11** | **associate Dot11** | **authentication** | **authfail Dot11** | **deauthenticate Dot11** | **disassociate Dot11** | **exclude**}{ **enable** | **disable**} command.

config logging syslog facility *Client*

Syntax Description

Client	Facility Client. Has the following functions: • assocfail Dot11—Association fail syslog for clients • associate Dot11—Association syslog for clients • authentication—Authentication success syslog for clients • authfail Dot11—Authentication fail syslog for clients • deauthenticate Dot11—Deauthentication syslog for clients • disassociate Dot11—Disassociation syslog for clients • excluded—Excluded syslog for clients

Command Default

None

Command History

Release	Modification
7.5	This command was introduced in a release earlier than Release 7.5.

The following example shows how to set the facility syslog facility for client:

```
cisco controller config logging syslog facility client
```

Related Commands

show logging flags client

config logging syslog facility ap

To configure the syslog facility to AP, use the **config logging syslog facility ap** { **associate** | **disassociate**} { **enable** | **disable**} command.

config logging syslog facility *AP*

Syntax Description

AP	Facility AP. Has the following functions: • associate—Association syslog for AP • disassociate—Disassociation syslog for AP

Command Default

None

Command History

Release	Modification
7.5	This command was introduced in a release earlier than Release 7.5.

The following example shows how to configure syslog facility for AP:

```
cisco controller config logging syslog facility ap
```

Related Commands

show logging flags ap

config logging syslog level

To set the severity level for filtering syslog messages to the remote host, use the **config logging syslog level** command.

config logging syslog level *severity_level*

Syntax Description

severity_level	Severity level. Choose one of the following: • 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

Command Default

None

Command History

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

The following example shows how to set the severity level for syslog messages to 3:

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

Related Commands

config logging syslog host

config logging syslog facility

show logging

config loginsession close

To close all active Telnet sessions, use the **config loginsession close** command.

config loginsession close {*session_id* | **all**}

Syntax Description

session_id	ID of the session to close.
all	Closes all Telnet sessions.

Command Default

None

Command History

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

The following example shows how to close all active Telnet sessions:

```
(Cisco Controller) > config loginsession close all
```

Related Commands

show loginsession

config mdns profile

To configure a multicast DNS (mDNS) profile and associate a service with the profile, use the **config mdns profile** command.

config mdns profile {**create** | **delete** | **service** {**add** | **delete**} *service _name profile_name*

Syntax Description

create	Creates an mDNS profile.
delete	Deletes an mDNS profile. If the profile is associated to an interface group, an interface, or a WLAN, an error appears.
service	Configures an mDNS service.
add	Adds an mDNS service to an mDNS profile.
delete	Deletes an mDNS service from an mDNS profile.
service -name	Name of the mDNS service.
profile_name	Name of the mDNS profile. You can create a maximum of 16 profiles.

Command Default

By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.

The following example shows how to add the Apple TV mDNS service to the mDNS profile1.

```
(Cisco Controller) > config mdns profile create profile1 Apple TV
```

Related Commands

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config mdns query interval

To configure the query interval for multicast DNS (mDNS) services, use the **config mdns query interval** command.

config mdns query interval *interval_value*

Syntax Description

interval_value	mDNS query interval, in minutes, that you can set. The query interval is the frequency at which the controller sends periodic queries to all the services defined in the Master Services database. The range is from 10 to 120.

Command Default

The default query interval for an mDNS service is 15 minutes.

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database. mDNS uses the multicast IP address 224.0.0.251 as the destination address and 5353 as UDP destination port.

The following example shows how to configure the query interval for mDNS services as 20 minutes.

```
(Cisco Controller) > config mdns query interval 20
```

Related Commands

config mdns profile

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config mdns service

To configure multicast DNS (mDNS) services in the master services database, use the **config mdns service** command.

config mdns service {**create** *service_name service_string* **query** {**enable** | **disable**} | **delete** *service_name* | **query** {**enable** | **disable**}}

Syntax Description

create	Adds a new mDNS service to the Master Services database.
service_name	Name of the mDNS service, for example, Air Tunes, iTunes Music Sharing, FTP, Apple File Sharing Protocol (AFP).
service_string	Unique string associated to an mDNS service, for example, _airplay._tcp.local. is the service string associated with Apple TV.
delete	Deletes an mDNS service from the Master Services database. Before deleting the service, the controller checks if any profile is using the service. **Note** You must delete the service from all profiles before deleting it.
query	Configures the query status for the mDNS service.
enable	Enables periodic query for an mDNS service by the controller.
disable	Disables periodic query for an mDNS service by the controller.

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database. The controller can snoop and learn a maximum of 64 services in Release 7.4.

Related Topics

config wlan mdns
config mdns profile, on page 179
config mdns query interval, on page 181
config mdns snooping , on page 183
clear mdns service-database, on page 26
debug mdns all, on page 506
debug mdns detail , on page 507
debug mdns error , on page 507
debug mdns message , on page 508
show mdns profile, on page 427
show mdns service , on page 429

config mdns snooping

To enable or disable global multicast DNS (mDNS) snooping on the Cisco WLC, use the **config mdns snooping** command.

config mdns snooping {**enable** | **disable**}

Syntax Description

enable	Enables mDNS snooping on the Cisco WLC.
disable	Disables mDNS snooping on the Cisco WLC.

Command Default

By default, mDNS snooping is enabled on the Cisco WLC.

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

mDNS service discovery provides a way to announce and discover services on the local network. mDNS perform DNS queries over IP multicast. mDNS supports zero configuration IP networking.

The following example shows how to enable mDNS snooping:

```
(Cisco Controller) > config mdns snooping enable
```

Related Commands

config mdns query interval

config mdns service

config mdns profile

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config mdns policy enable

To configure the mDNS policy use the **config mdns policy enable | disable** command.

config mdnspolicyenable | disable

Syntax Description

policy	Name of the mDNS policy.
enable	Enables the policy for an mDNS service by the controller.
disable	Disables the policy for an mDNS service by the controller.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

This command is valid for 8.0 release onwards.

Example

The following example show how to configure the mDNS policy.

```
(Cisco Controller) >config mdns
  policy enable
```

config mdns policy service-group

To create or delete mDNS policy service group use the **config mdns policy service-group** command.

config mdns policy service-group {**create** | **delete**} *service-group-name*

Syntax Description

create	Creates the mDNS service group.
delete	Deletes the mDNS service group.
service-group-name	Name of the service group.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Example

The following example shows how to delete a mDNS service group.

```
(Cisco Controller) >config mdns policy service-group create <service-group-name>
```

config mdns policy service-group parameters

To configure the parameters of a service group, use the **config mdns policy service-group** command.

config mdnspolicyservice-group device-mac add *service-group-name mac-addr device name* **location-type** *[AP_LOCATION | AP_NAME |AP_GROUP]* **device-location** *[location string |any | same]*

Syntax Description

device-mac	Configures MAC address of a service provider device.
add	Adds the service group name of the service provider device.
service-group-name	Name of a mDNS service group.
device-name	Name of a device to which the service provider belongs.
location type	Configures a location type of a service provider device.
[AP_LOCATION | AP_NAME | AP_GROUP]	Name, location, group of the access point.
device-location	Configures location of a device to which the service provider belongs.
[location string |any | same]	location string of a device.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Example

The following example shows how to configure a location type of a service provider device.

```
(Cisco Controller) >config mdns policy service-group location type [AP_LOCATION | AP_NAME
| AP_GROUP]
```

config mdns policy service-group user-name

To configure a user role for a mDNS service group, use the **config mdns policy service-group user-name add | delete <service-group-name> <user-role-name>**command

config mdnspolicyservice-groupuser-nameadd | delete*service-group-name user-name*

Syntax Description

user-name	Configures name of a user for mDNS service group.
service-group-name	Name of a mDNS service group
user-name	Name of the user role for mDNS service group

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Example

The following example show how to add user name for a mDNS service group

```
(Cisco Controller) >config mdns policy service-group user-name add <service-group-name>
<user-role-name>
```

config mdns policy service-group user-role

To configure a user role for a mDNS service group, use the **config mdns policy service-group user-role add | delete <service-group-name> <user-role-name>**command.

config mdnspolicyservice-groupuser-roleadd | delete*service-group-name user-role-name*

Syntax Description

user-role	Configures a user role for mDNS service group.
service-group-name	Name of a mDNS service group
user-role-name	Name of the user role for mDNS service group

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Example

The following example show how to add user role details for a mDNS service group

```
(Cisco Controller) >config mdns policy service-group user-role add <service-group-name>
<user-role-name>
```

config memory monitor errors

To enable or disable monitoring for memory errors and leaks, use the **config memory monitor errors** command.

config memory monitor errors {**enable** | **disable**}

Caution The **config memory monitor** commands can be disruptive to your system and should be run only when you are advised to do so by the Cisco TAC.

Syntax Description

enable	Enables the monitoring for memory settings.
disable	Disables the monitoring for memory settings.

Command Default

Monitoring for memory errors and leaks is disabled by default.

Command History

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

Usage Guidelines

Be cautious about changing the defaults for the **config memory monitor** command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

The following example shows how to enable monitoring for memory errors and leaks for a controller:

```
(Cisco Controller) > config memory monitor errors enable
```

Related Commands

config memory monitor leaks

debug memory

show memory monitor

config memory monitor leaks

To configure the controller to perform an auto-leak analysis between two memory thresholds, use the **config memory monitor leaks** command.

config memory monitor leaks *low_thresh high_thresh*

Caution The **config memory monitor** commands can be disruptive to your system and should be run only when you are advised to do so by the Cisco TAC.

Syntax Description

low_thresh	Value below which free memory cannot fall without crashing. This value cannot be set lower than 10000 KB.
high_thresh	Value below which the controller enters auto-leak-analysis mode. See the "Usage Guidelines" section.

Command Default

The default value for *low_thresh* is 10000 KB; the default value for *high_thresh* is 30000 KB.

Command History

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

Usage Guidelines

Note Be cautious about changing the defaults for the **config memory monitor** command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

Use this command if you suspect that a memory leak has occurred.

If the free memory is lower than the *low_thresh* threshold, the system crashes, generating a crash file. The default value for this parameter is 10000 KB, and you cannot set it below this value.

Set the *high_thresh* threshold to the current free memory level or higher so that the system enters auto-leak-analysis mode. After the free memory reaches a level lower than the specified *high_thresh* threshold, the process of tracking and freeing memory allocation begins. As a result, the **debug memory events enable** command shows all allocations and frees, and the **show memory monitor detail** command starts to detect any suspected memory leaks.

The following example shows how to set the threshold values for auto-leak-analysis mode to 12000 KB for the low threshold and 35000 KB for the high threshold:

```
(Cisco Controller) > config memory monitor leaks 12000 35000
```

Related Commands

config memory monitor leaks

debug memory

show memory monitor

config mgmtuser add

To add a local management user to the controller, use the **config mgmtuser add** command.

config mgmtuser add *username password* {**lobby-admin** | **read-write** | **read-only**} [*description*]

Syntax Description

username	Account username. The username can be up to 24 alphanumeric characters.
password	Account password. The password can be up to 24 alphanumeric characters.
read-write	Creates a management user with read-write access.
read-only	Creates a management user with read-only access.
description	(Optional) Description of the account. The description can be up to 32 alphanumeric characters within double quotes.

Command Default

None

Command History

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

The following example shows how to create a management user account with read-write access.

```
(Cisco Controller) > config mgmtuser add admin admin read-write "Main account"
```

Related Commands

show mgmtuser

config mgmtuser delete

To delete a management user from the controller, use the **config mgmtuser delete** command.

config mgmtuser delete *username*

Syntax Description

username	Account username. The username can be up to 24 alphanumeric characters.

Command Default

The management user is not deleted by default.

Command History

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

The following example shows how to delete a management user account admin from the controller.

```
(Cisco Controller) > config mgmtuser delete admin

Deleted user admin
```

Related Commands

show mgmtuser

config mgmtuser description

To add a description to an existing management user login to the controller, use the **config mgmtuser description** command.

config mgmtuser description *username description*

Syntax Description

username	Account username. The username can be up to 24 alphanumeric characters.
description	Description of the account. The description can be up to 32 alphanumeric characters within double quotes.

Command Default

No description is added to the management user.

Command History

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

The following example shows how to add a description “primary-user” to the management user “admin”:

```
(Cisco Controller) > config mgmtuser description admin "primary-user"
```

Related Commands

config mgmtuser add

config mgmtuser delete

config mgmtuser password

show mgmtuser

config mgmtuser password

To configure a management user password, use the **config mgmtuser password** command.

config mgmtuser password *username password*

Syntax Description

username	Account username. The username can be up to 24 alphanumeric characters.
password	Account password. The password can be up to 24 alphanumeric characters.

Command Default

None

Command History

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

The following example shows how to change the password of the management user “admin” with the new password 5rTfm:

```
(Cisco Controller) > config mgmtuser password admin 5rTfm
```

Related Commands

show mgmtuser

config mobility group member

To add or delete users from the mobility group member list, use the **config mobility group member** command.

config mobility group member {**add** *MAC-addr IP-addr* [*group_name*] [**encrypt**{**enable** | **disable**] | [**data-dtls** *mac-addr* {**enable** | **disable**} | **delete** *MAC-addr* | **hash** *IP-addr* {*key* | **none**}}

Syntax Description

add	Adds or changes a mobility group member to the list.
MAC-addr	Member switch MAC address.
IP-addr	Member switch IP address.
group_name	(Optional) Member switch group name (if different from the default group name).
delete	(Optional) Deletes a mobility group member from the list.
hash	Configures the hash key for authorization. You can configure the hash key only if the member is a virtual controller in the same domain.
key	Hash key of the virtual controller. For example, a819d479dcfeb3e0974421b6e8335582263d9169
none	Clears the previous hash key of the virtual controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.
8.8.111.0	This command was updated by adding **encrypt** , **data-dtls** keywords to support IRCM functionality.

The following example shows how to add a mobility group member with an IPv4 address to the list:

```
(Cisco Controller) >config mobility group member add 11:11:11:11:11:11 209.165.200.225
```

The following example shows how to configure the hash key of a virtual controller in the same domain:

```
(Cisco Controller) >config mobility group member hash 209.165.201.1
a819d479dcfeb3e0974421b6e8335582263d9169
```

config netuser add

To add a guest user on a WLAN or wired guest LAN to the local user database on the controller, use the **config netuser add** command.

config netuser add *username password* {**wlan** *wlan_id* | **guestlan** *guestlan_id*} **userType guest lifetime** *lifetime* **description** *description*

Syntax Description

username	Guest username. The username can be up to 50 alphanumeric characters.
password	User password. The password can be up to 24 alphanumeric characters.
wlan	Specifies the wireless LAN identifier to associate with or zero for any wireless LAN.
wlan_id	Wireless LAN identifier assigned to the user. A zero value associates the user with any wireless LAN.
guestlan	Specifies the guest LAN identifier to associate with or zero for any wireless LAN.
guestlan_id	Guest LAN ID.
userType	Specifies the user type.
guest	Specifies the guest for the guest user.
lifetime	Specifies the lifetime.
lifetime	Lifetime value (60 to 259200 or 0) in seconds for the guest user. **Note** A value of 0 indicates an unlimited lifetime.
description	Short description of user. The description can be up to 32 characters enclosed in double-quotes.

Command Default

None

Command History

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

Usage Guidelines

Local network usernames must be unique because they are stored in the same database.

The following example shows how to add a permanent username Jane to the wireless network for 1 hour:

```
(Cisco Controller) > config netuser add jane able2 1 wlan_id 1 userType permanent
```

The following example shows how to add a guest username George to the wireless network for 1 hour:

```
(Cisco Controller) > config netuser add george able1 guestlan 1 3600
```

Related Commands

show netuser

config netuser delete

config netuser delete

To delete an existing user from the local network, use the **config netuser delete** command.

config netuser delete *username*

Syntax Description

username	Network username. The username can be up to 24 alphanumeric characters.

Command Default

None

Command History

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

Usage Guidelines

Local network usernames must be unique because they are stored in the same database.

The following example shows how to delete an existing username named able1 from the network:

```
(Cisco Controller) > config netuser delete able1
Deleted user able1
```

Related Commands

show netuser

config netuser description

To add a description to an existing net user, use the **config netuser description** command.

config netuser description *username description*

Syntax Description

username	Network username. The username can contain up to 24 alphanumeric characters.
description	(Optional) User description. The description can be up to 32 alphanumeric characters enclosed in double quotes.

Command Default

None

Command History

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

The following example shows how to add a user description “HQ1 Contact” to an existing network user named able 1:

```
(Cisco Controller) > config netuser description able1 “HQ1 Contact”
```

Related Commands

show netuser

config netuser guest-lan-id

To configure a wired guest LAN ID for a network user, use the **config netuser guest-lan-id** command.

config netuser guest-lan-id *username lan_id*

Syntax Description

username	Network username. The username can be 24 alphanumeric characters.
lan_id	Wired guest LAN identifier to associate with the user. A zero value associates the user with any wired LAN.

Command Default

None

Command History

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

The following example shows how to configure a wired LAN ID 2 to associate with the user named aire1:

```
(Cisco Controller) > config netuser guest- lan-id aire1 2
```

Related Commands

show netuser

show wlan summary

config netuser guest-role apply

To apply a quality of service (QoS) role to a guest user, use the **config netuser guest-role apply** command.

config netuser guest-role apply *username role_name*

Syntax Description

username	Name of the user.
role_name	QoS guest role name.

Command Default

None

Command History

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

Usage Guidelines

If you do not assign a QoS role to a guest user, the Role field in the User Details shows the role as default. The bandwidth contracts for this user are defined in the QoS profile for the WLAN.

If you want to unassign a QoS role from a guest user, use the **config netuser guest-role apply** *username* **default**. This user now uses the bandwidth contracts defined in the QoS profile for the WLAN.

The following example shows how to apply a QoS role to a guest user jsmith with the QoS guest role named Contractor:

```
(Cisco Controller) > config netuser guest-role apply jsmith Contractor
```

Related Commands

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role create

To create a quality of service (QoS) role for a guest user, use the **config netuser guest-role create** command.

config netuser guest-role create *role_name*

Syntax Description

role name	QoS guest role name.

Command Default

None

Command History

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

Usage Guidelines

To delete a QoS role, use the **config netuser guest-role delete** *role-name* .

The following example shows how to create a QoS role for the guest user named guestuser1:

```
(Cisco Controller) > config netuser guest-role create guestuser1
```

Related Commands

config netuser guest-role delete

config netuser guest-role delete

To delete a quality of service (QoS) role for a guest user, use the **config netuser guest-role delete** command.

config netuser guest-role delete *role_name*

Syntax Description

role name	Quality of service (QoS) guest role name.

Command Default

None

Command History

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

The following example shows how to delete a quality of service (QoS) role for guestuser1:

```
(Cisco Controller) > config netuser guest-role delete guestuser1
```

Related Commands

config netuser guest-role create

config netuser guest-role qos data-rate average-data-rate

To configure the average data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate average-data-rate** command.

config netuser guest-role qos data-rate average-data-rate *role_name rate*

Syntax Description

role_name	Quality of service (QoS) guest role name.
rate	Rate for TCP traffic on a per user basis.

Command Default

None

Usage Guidelines

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure an average rate for the QoS guest named guestuser1:

```
(Cisco Controller) > config netuser guest-role qos data-rate average-data-rate guestuser1
0
```

Related Commands

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role qos data-rate burst-data-rate

config netuser guest-role qos data-rate average-realtime-rate

To configure the average data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate average-realtime-rate** command.

config netuser guest-role qos data-rate average-realtime-rate *role_name rate*

Syntax Description

role_name	Quality of service (QoS) guest role name.
rate	Rate for TCP traffic on a per user basis.

Command Default

None

Usage Guidelines

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure an average data rate for the QoS guest user named guestuser1 with the rate for TCP traffic of 0 Kbps:

```
(Cisco Controller) > config netuser guest-role qos data-rate average-realtime-rate guestuser1
 0
```

Related Commands

config netuser guest-role

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-data-rate

To configure the peak data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate burst-data-rate** command.

config netuser guest-role qos data-rate burst-data-rate *role_name rate*

Syntax Description

role_name	Quality of service (QoS) guest role name.
rate	Rate for TCP traffic on a per user basis.

Command Default

None

Command History

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

Usage Guidelines

The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure the peak data rate for the QoS guest named guestuser1 with the rate for TCP traffic of 0 Kbps:

```
(Cisco Controller) > config netuser guest-role qos data-rate burst-data-rate guestuser1 0
```

Related Commands

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-realtime-rate

To configure the burst real-time data rate for UDP traffic on a per user basis, use the **config netuser guest-role qos data-rate burst-realtime-rate** command.

config netuser guest-role qos data-rate burst-realtime-rate *role_name rate*

Syntax Description

role_name	Quality of service (QoS) guest role name.
rate	Rate for TCP traffic on a per user basis.

Command Default

None

Command History

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

Usage Guidelines

The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the quality of service (QoS) policy may block traffic to and from the wireless client.

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure a burst real-time rate for the QoS guest user named guestuser1 with the rate for TCP traffic of 0 Kbps:

```
(Cisco Controller) > config netuser guest-role qos data-rate burst-realtime-rate guestuser1
 0
```

Related Commands

config netuser guest-role

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-data-rate

config netuser lifetime

To configure the lifetime for a guest network user, use the **config netuser lifetime** command.

config netuser lifetime *username time*

Syntax Description

username	Network username. The username can be up to 50 alphanumeric characters.
time	Llifetime between 60 to 31536000 seconds or 0 for no limit.

Command Default

None

Command History

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

The following example shows how to configure lifetime for a guest network user:

```
(Cisco Controller) > config netuser lifetime guestuser1 22450
```

Related Commands

show netuser

show wlan summary

config netuser maxUserLogin

To configure the maximum number of login sessions allowed for a network user, use the **config netuser maxUserLogin** command.

config netuser maxUserLogin *count*

Syntax Description

count	Maximum number of login sessions for a single user. The allowed values are from 0 (unlimited) to 8.

Command Default

By default, the maximum number of login sessions for a single user is 0 (unlimited).

Command History

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

The following example shows how to configure the maximum number of login sessions for a single user to 8:

```
(Cisco Controller) > config netuser maxUserLogin 8
```

Related Commands

show netuser

config netuser password

To change a local network user password, use the **config netuser password** command.

config netuser password *username password*

Syntax Description

username	Network username. The username can be up to 24 alphanumeric characters.
password	Network user password. The password can contain up to 24 alphanumeric characters.

Command Default

None

Command History

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

The following example shows how to change the network user password from aire1 to aire2:

```
(Cisco Controller) > config netuser password aire1 aire2
```

Related Commands

show netuser

config netuser wlan-id

To configure a wireless LAN ID for a network user, use the **config netuser wlan-id** command.

config netuser wlan-id *username wlan_id*

Syntax Description

username	Network username. The username can be 24 alphanumeric characters.
wlan_id	Wireless LAN identifier to associate with the user. A zero value associates the user with any wireless LAN.

Command Default

None

Command History

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

Examples

The following example shows how to configure a wireless LAN ID 2 to associate with the user named aire1:

```
(Cisco Controller) > config netuser wlan-id aire1 2
```

Related Commands

show netuser

show wlan summary

config network 802.3-bridging

To enable or disable 802.3 bridging on a controller, use the **config network 802.3-bridging** command.

config network 802.3-bridging {**enable** | **disable**}

Syntax Description

enable	Enables the 802.3 bridging.
disable	Disables the 802.3 bridging.

Command Default

By default, 802.3 bridging on the controller is disabled.

Command History

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

Usage Guidelines

In controller software release 5.2, the software-based forwarding architecture for Cisco 2100 Series Controllers is being replaced with a new forwarding plane architecture. As a result, Cisco 2100 Series Controllers and the Cisco wireless LAN controller Network Module for Cisco Integrated Services Routers bridge 802.3 packets by default. Therefore, 802.3 bridging can now be disabled only on Cisco 4400 Series Controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch.

To determine the status of 802.3 bridging, enter the **show netuser guest-roles** command.

The following example shows how to enable the 802.3 bridging:

```
(Cisco Controller) > config network 802.3-bridging enable
```

Related Commands

show netuser guest-roles

show network

config network allow-old-bridge-aps

To configure an old bridge access point's ability to associate with a switch, use the **config network allow-old-bridge-aps** command.

config network allow-old-bridge-aps {**enable** | **disable**}

Syntax Description

enable	Enables the switch association.
disable	Disables the switch association.

Command Default

Switch association is enabled.

Command History

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

The following example shows how to configure an old bridge access point to associate with the switch:

```
(Cisco Controller) > config network allow-old-bridge-aps enable
```

config network ap-discovery

To enable or disable NAT IP in an AP discovery response, use the **config network ap-discovery** command.

config network ap-discovery nat-ip-only {**enable** | **disable**}

Syntax Description

enable	Enables use of NAT IP only in discovery response.
disable	Enables use of both NAT IP and non NAT IP in discovery response.

Command Default

The use of NAT IP only in discovery response is enabled.

Command History

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

Usage Guidelines

- If the **config interface nat-address management** command is set, this command controls which address(es) are sent in the CAPWAP discovery responses.
- If all APs are on the outside of the NAT gateway of the controller, enter the **config network ap-discovery nat-ip-only enable** command, and only the management NAT address is sent.
- If the controller has both APs on the outside and the inside of its NAT gateway, enter the **config network ap-discovery nat-ip-only disable** command, and both the management NAT address and the management inside address are sent. Ensure that you have entered the **config ap link-latency disable all** command to avoid stranding APs.
- If you disable **nat-ip-only**, the controller sends all active AP-Manager interfaces with their non-NAT IP in discovery response to APs.

  If you enable **nat-ip-only**, the controller sends all active AP-Manager interfaces with NAT IP if configured for the interface, else non-NAT IP.

  We recommend that you configure the interface as AP-Manager interface with NAT IP or non-NAT IP keeping these scenarios in mind because the AP chooses the least loaded AP-Manager interface received in the discovery response.

The following example shows how to enable NAT IP in an AP discovery response:

```
(Cisco Controller) > config network ap-discovery nat-ip-only enable
```

config network ap-fallback

To configure Cisco lightweight access point fallback, use the **config network ap-fallback** command.

config network ap-fallback {**enable** | **disable**}

Syntax Description

enable	Enables the Cisco lightweight access point fallback.
disable	Disables the Cisco lightweight access point fallback.

Command Default

The Cisco lightweight access point fallback is enabled.

Command History

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

The following example shows how to enable the Cisco lightweight access point fallback:

```
(Cisco Controller) > config network ap-fallback enable
```

config network ap-priority

To enable or disable the option to prioritize lightweight access points so that after a controller failure they reauthenticate by priority rather than on a first-come-until-full basis, use the **config network ap-priority** command.

config network ap-priority {**enable** | **disable**}

Syntax Description

enable	Enables the lightweight access point priority reauthentication.
disable	Disables the lightweight access point priority reauthentication.

Command Default

The lightweight access point priority reauthentication is disabled.

Command History

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

The following example shows how to enable the lightweight access point priority reauthorization:

```
(Cisco Controller) > config network ap-priority enable
```

config network apple-talk

To configure AppleTalk bridging, use the **config network apple-talk** command.

config network apple-talk {**enable** | **disable**}

Syntax Description

enable	Enables the AppleTalk bridging.
disable	Disables the AppleTalk bridging.

Command Default

None

Command History

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

The following example shows how to configure AppleTalk bridging:

```
(Cisco Controller) > config network apple-talk enable
```

config network arptimeout

To set the Address Resolution Protocol (ARP) entry timeout value, use the **config network arptimeout** command.

config network arptimeout *seconds*

Syntax Description

seconds	Timeout in seconds. The minimum value is 10 seconds. The default value is 300 seconds.

Command Default

The default ARP entry timeout value is 300 seconds.

Command History

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

This example shows how to set the ARP entry timeout value to 240 seconds:

```
(Cisco Controller) > config network arptimeout 240
```

Related Commands

show network summary

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

config network bridging-shared-secret *shared_secret*

Syntax Description

shared_secret	Bridging shared secret string. The string can contain up to 10 bytes.

Command Default

The bridging shared secret is enabled by default.

Command History

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

Usage Guidelines

This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.

The zero-touch configuration must be enabled for this command to work.

The following example shows how to configure the bridging shared secret string “shhh1”:

```
(Cisco Controller) > config network bridging-shared-secret shhh1
```

Related Commands

show network summary

config network broadcast

To enable or disable broadcast packet forwarding, use the **config network broadcast** command.

config network broadcast {**enable** | **disable**}

Syntax Description

enable	Enables the broadcast packet forwarding.
disable	Disables the broadcast packet forwarding.

Command Default

The broadcast packet forwarding is disabled by default.

Command History

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

Usage Guidelines

This command allows you to enable or disable broadcasting. You must enable multicast mode before enabling broadcast forwarding. Use the **config network multicast mode command** to configure multicast mode on the controller.

Note The default multicast mode is unicast in case of all controllers except for Cisco 2106 Controllers. The broadcast packets and multicast packets can be independently controlled. If multicast is off and broadcast is on, broadcast packets still reach the access points, based on the configured multicast mode.

The following example shows how to enable broadcast packet forwarding:

```
(Cisco Controller) > config network broadcast enable
```

Related Commands

show network summary

config network multicast global

config network multicast mode

config network fast-ssid-change

To enable or disable fast Service Set Identifier (SSID) changing for mobile stations, use the **config network fast-ssid-change** command.

config network fast-ssid-change {**enable** | **disable**}

Syntax Description

enable	Enables the fast SSID changing for mobile stations
disable	Disables the fast SSID changing for mobile stations.

Command Default

None

Command History

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

Usage Guidelines

When you enable the Fast SSID Change feature, the controller allows clients to move between SSIDs. When the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID.

When you disable the FastSSID Change feature, the controller enforces a delay before clients are allowed to move to a new SSID.

The following example shows how to enable the fast SSID changing for mobile stations:

```
(Cisco Controller) > config network fast-ssid-change enable
```

Related Commands

show network summary

config network ip-mac-binding

To validate the source IP address and MAC address binding within client packets, use the **config network ip-mac-binding** command.

config network ip-network-binding {**enable** | **disable**}

Syntax Description

enable	Enables the validation of the source IP address to MAC address binding in clients packets.
disable	Disables the validation of the source IP address to MAC address binding in clients packets.

Command Default

The validation of the source IP address to MAC address binding in clients packets is enabled by default.

Command History

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

Usage Guidelines

In controller software release 5.2, the controller enforces strict IP address-to-MAC address binding in client packets. The controller checks the IP address and MAC address in a packet, compares them to the addresses that are registered with the controller, and forwards the packet only if they both match. In previous releases, the controller checks only the MAC address of the client and ignores the IP address.

Note You might want to disable this binding check if you have a routed network behind a workgroup bridge (WGB).

The following example shows how to validate the source IP and MAC address within client packets:

```
(Cisco Controller) > config network ip-mac-binding enable
```

config network master-base

To enable or disable the Cisco wireless LAN controller as an access point default primary, use the **config network master-base** command.

config network master-base {**enable** | **disable**}

Syntax Description

enable	Enables the Cisco wireless LAN controller acting as a Cisco lightweight access point default primary.
disable	Disables the Cisco wireless LAN controller acting as a Cisco lightweight access point default primary.

Command Default

None

Command History

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

Usage Guidelines

This setting is only used upon network installation and should be disabled after the initial network configuration. Because the primary Cisco wireless LAN controller is normally not used in a deployed network, the primary Cisco wireless LAN controller setting can be saved from 6.0.199.0 or later releases.

The following example shows how to enable the Cisco wireless LAN controller as a default primary:

```
(Cisco Controller) > config network master-base enable
```

config network mgmt-via-wireless

To enable Cisco wireless LAN controller management from an associated wireless client, use the **config network mgmt-via-wireless** command.

config network mgmt-via-wireless {**enable** | **disable**}

Syntax Description

enable	Enables the switch management from a wireless interface.
disable	Disables the switch management from a wireless interface.

Command Default

The switch management from a wireless interface is disabled by default.

Command History

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

Usage Guidelines

This feature allows wireless clients to manage only the Cisco wireless LAN controller associated with the client and the associated Cisco lightweight access point. That is, clients cannot manage another Cisco wireless LAN controller with which they are not associated.

This example shows how to configure switch management from a wireless interface:

```
(Cisco Controller) > config network mgmt-via-wireless enable
```

Related Commands

show network summary

config network multicast global

To enable or disable multicasting on the controller, use the **config network multicast global** command.

config network multicast global {**enable** | **disable**}

Syntax Description

enable	Enables the multicast global support.
disable	Disables the multicast global support.

Command Default

Multicasting on the controller is disabled by default.

Command History

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

Usage Guidelines

The **config network broadcast** {**enable** | **disable**} command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. This command uses the multicast mode configured on the controller (by using the **config network multicast mode command)** to operate.

The following example shows how to enable the global multicast support:

```
(Cisco Controller) > config network multicast global enable
```

Related Commands

show network summary

config network broadcast

config network multicast mode

config network multicast igmp query interval

To configure the IGMP query interval, use the **config network multicast igmp query interval** command.

config network multicast igmp query interval *value*

Syntax Description

value	Frequency at which controller sends IGMP query messages. The range is from 15 to 2400 seconds.

Command Default

The default IGMP query interval is 20 seconds.

Command History

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

Usage Guidelines

To configure IGMP query interval, ensure that you do the following:

- Enable the global multicast by entering the **config network multicast global enable** command.
- Enable IGMP snooping by entering the **config network multicast igmp snooping enable** command.

The following example shows how to configure the IGMP query interval at 20 seconds:

```
(Cisco Controller) > config network multicast igmp query interval 20
```

Related Commands

config network multicast global

config network multicast igmp snooping

config network multicast igmp timeout

config network multicast igmp snooping

To enable or disable IGMP snooping, use the **config network multicast igmp snooping** command.

config network multicast igmp snooping {**enable** | **disable**}

Syntax Description

enable	Enables IGMP snooping.
disable	Disables IGMP snooping.

Command Default

None

Command History

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

The following example shows how to enable internet IGMP snooping settings:

```
(Cisco Controller) > config network multicast igmp snooping enable
```

Related Commands

config network multicast global

config network multicast igmp query interval

config network multicast igmp timeout

config network multicast igmp timeout

To set the IGMP timeout value, use the **config network multicast igmp timeout** command.

config network multicast igmp timeout *value*

Syntax Description

value	Timeout range from 30 to 7200 seconds.

Command Default

None

Command History

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

Usage Guidelines

You can enter a timeout value between 30 and 7200 seconds. The controller sends three queries in one timeout value at an interval of timeout/3 to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

The following example shows how to configure the timeout value 50 for IGMP network settings:

```
(Cisco Controller) > config network multicast igmp timeout 50
```

Related Commands

config network multicast global

config network igmp snooping

config network multicast igmp query interval

config network multicast l2mcast

To configure the Layer 2 multicast on an interface or all interfaces, use the **config network multicast l2mcast** command.

config network multicast l2mcast {**enable** | **disable** {**all** | *interface-name*}

Syntax Description

enable	Enables Layer 2 multicast.
disable	Disables Layer 2 multicast.
all	Applies to all interfaces.
interface-name	Interface name for which the Layer 2 multicast is to enabled or disabled.

Command Default

None

Command History

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

The following example shows how to enable Layer 2 multicast for all interfaces:

```
(Cisco Controller) > config network multicast l2mcast enable all
```

Related Commands

config network multicast global

config network multicast igmp snooping

config network multicast igmp query interval

config network multicast mld

config network multicast mld

To configure the Multicast Listener Discovery (MLD) parameters, use the **config network multicast mld** command.

config network multicast mld {**query interval** *interval-value* | **snooping** {**enable** | **disable**} | **timeout** *timeout-value*}

Syntax Description

query interval	Configures query interval to send MLD query messages.
interval-value	Query interval in seconds. The range is from 15 to 2400 seconds.
snooping	Configures MLD snooping.
enable	Enables MLD snooping.
disable	Disables MLD snooping.
timeout	Configures MLD timeout.
timeout-value	Timeout value in seconds. The range is from 30 seconds to 7200 seconds.

Command Default

None

Command History

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

The following example shows how to set a query interval of 20 seconds for MLD query messages:

```
(Cisco Controller) > config network multicast mld query interval 20
```

Related Commands

config network multicast global

config network multicast igmp snooping

config network multicast igmp query interval

config network multicast l2mcast

config network multicast mode multicast

To configure the controller to use the multicast method to send broadcast or multicast packets to an access point, use the **config network multicast mode multicast** command.

config network multicast mode multicast

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to configure the multicast mode to send a single copy of data to multiple receivers:

```
(Cisco Controller) > config network multicast mode multicast
```

Related Commands

config network multicast global

config network broadcast

config network multicast mode unicast

config network multicast mode unicast

To configure the controller to use the unicast method to send broadcast or multicast packets to an access point, use the **config network multicast mode unicast** command.

config network multicast mode unicast

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to configure the controller to use the unicast mode:

```
(Cisco Controller) > config network multicast mode unicast
```

Related Commands

config network multicast global

config network broadcast

config network multicast mode multicast

config network oeap-600 dual-rlan-ports

To configure the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4, use the **config network oeap-600 dual-rlan-ports** command.

config network oeap-600 dual-rlan-ports {**enable** | **disable**}

Syntax Description

enable	Enables Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4.
disable	Resets the Ethernet port 3 Cisco OfficeExtend 600 Series access points to function as a local LAN port.

Command Default

The Ethernet port 3 Cisco 600 Series OEAP is reset.

Command History

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

The following example shows how to enable the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port:

```
(Cisco Controller) > config network oeap-600 dual-rlan-ports enable
```

config network oeap-600 local-network

To configure access to the local network for the Cisco 600 Series OfficeExtend access points, use the **config network oeap-600 local-network** command.

config network oeap-600 local-network {**enable** | **disable**}

Syntax Description

enable	Enables access to the local network for the Cisco 600 Series OfficeExtend access points.
disable	Disables access to the local network for the Cisco 600 Series OfficeExtend access points.

Command Default

Access to the local network for the Cisco 600 Series OEAPs is disabled.

Command History

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

The following example shows how to enable access to the local network for the Cisco 600 Series OfficeExtend access points:

```
(Cisco Controller) > config network oeap-600 local-network enable
```

config network otap-mode

To enable or disable over-the-air provisioning (OTAP) of Cisco lightweight access points, use the **config network otap-mode** command.

config network otap-mode {**enable** | **disable**}

Syntax Description

enable	Enables the OTAP provisioning.
disable	Disables the OTAP provisioning.

Command Default

The OTAP provisioning is enabled.

Command History

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

The following example shows how to disable the OTAP provisioning:

```
(Cisco Controller) >config network otap-mode disable
```

config network rf-network-name

To set the RF-Network name, use the **config network rf-network-name** command.

config network rf-network-name *name*

Syntax Description

name	RF-Network name. The name can contain up to 19 characters.

Command Default

None

Command History

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

The following example shows how to set the RF-network name to travelers:

```
(Cisco Controller) > config network rf-network-name travelers
```

Related Commands

show network summary

Related Topics

debug airewave-director

config network secureweb

To change the state of the secure web (https is http and SSL) interface for management users, use the **config network secureweb** command.

config network secureweb {**enable** | **disable**}

Syntax Description

enable	Enables the secure web interface for management users.
disable	Disables the secure web interface for management users.

Command Default

The secure web interface for management users is enabled by default.

Command History

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

Usage Guidelines

This command allows management users to access the controller GUI using an http://ip-address. Web mode is not a secure connection.

The following example shows how to enable the secure web interface settings for management users:

```
(Cisco Controller) > config network secureweb enable
You must reboot for the change to take effect.
```

Related Commands

config network secureweb cipher-option

show network summary

config network secureweb cipher-option

To enable or disable secure web mode with increased security, or to enable or disable Secure Sockets Layer (SSL v2) for web administration and web authentication, use the **config network secureweb cipher-option** command.

config network secureweb cipher-option {**high** | **sslv2** | **rc4-preference**} {**enable** | **disable**}

Syntax Description

high	Configures whether or not 128-bit ciphers are required for web administration and web authentication.
sslv2	Configures SSLv2 for both web administration and web authentication.
rc4-preference	Configures preference for RC4-SHA (Rivest Cipher 4-Secure Hash Algorithm) cipher suites (over CBC cipher suites) for web authentication and web administration.
enable	Enables the secure web interface.
disable	Disables the secure web interface.

Command Default

The default is **disable** for secure web mode with increased security and **enable** for SSL v2.

Command History

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

Usage Guidelines

Note The **config network secureweb cipher-option** command allows users to access the controller GUI using an http://ip-address but only from browsers that support 128-bit (or larger) ciphers.

When cipher-option sslv2 is disabled, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later.

In RC4-SHA based cipher suites, RC4 is used for encryption and SHA is used for message authentication.

The following example shows how to enable secure web mode with increased security:

```
(Cisco Controller) > config network secureweb cipher-option
```

The following example shows how to disable SSL v2:

```
(Cisco Controller) > config network secureweb cipher-option sslv2 disable
```

Related Commands **config network secureweb**

show network summary

config network ssh

To allow or disallow new Secure Shell (SSH) sessions, use the **config network ssh** command.

config network ssh {**enable** | **disable**}

Syntax Description

enable	Allows the new SSH sessions.
disable	Disallows the new SSH sessions.

Command Default

The default value for the new SSH session is **disable**.

The following example shows how to enable the new SSH session:

```
(Cisco Controller) > config network ssh enable
```

Related Commands

show network summary

config network telnet

To allow or disallow new Telnet sessions, use the **config network telnet** command.

config network telnet {**enable** | **disable**}

Syntax Description

enable	Allows new Telnet sessions.
disable	Disallows new Telnet sessions.

Command Default

By default, the new Telnet session is disallowed and the value is **disable**.

Usage Guidelines

Telnet is not supported on Cisco Aironet 1830 and 1850 Series Access Points.

Command History

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

The following example shows how to configure the new Telnet sessions:

```
(Cisco Controller) > config network telnet enable
```

Related Commands

config ap telnet

show network summary

config network usertimeout

To change the timeout for idle client sessions, use the **config network usertimeout** command.

config network usertimeout *seconds*

Syntax Description

seconds	Timeout duration in seconds. The minimum value is 90 seconds. The default value is 300 seconds.

Command Default

The default timeout value for idle client session is 300 seconds.

Usage Guidelines

Use this command to set the idle client session duration on the Cisco wireless LAN controller. The minimum duration is 90 seconds.

The following example shows how to configure the idle session timeout to 1200 seconds:

```
(Cisco Controller) > config network usertimeout 1200
```

Related Commands

show network summary

config network web-auth captive-bypass

To configure the controller to support bypass of captive portals at the network level, use the **config network web-auth captive-bypass** command.

config network web-auth captive-bypass {**enable** | **disable**}

Syntax Description

enable	Allows the controller to support bypass of captive portals.
disable	Disallows the controller to support bypass of captive portals.

Command Default

None

The following example shows how to configure the controller to support bypass of captive portals:

```
(Cisco Controller) > config network web-auth captive-bypass enable
```

Related Commands

show network summary

config network web-auth cmcc-support

config network web-auth cmcc-support

To configure eWalk on the controller, use the **config network web-auth cmcc-support** command.

config network web-auth cmcc-support {**enable** | **disable**}

Syntax Description

enable	Enables eWalk on the controller.
disable	Disables eWalk on the controller.

Command Default

None

The following example shows how to enable eWalk on the controller:

```
(Cisco Controller) > config network web-auth cmcc-support enable
```

Related Commands

show network summary

config network web-auth captive-bypass

config network web-auth port

To configure an additional port to be redirected for web authentication at the network level, use the **config network web-auth port** command.

config network web-auth port *port*

Syntax Description

port	Port number. The valid range is from 0 to 65535.

Command Default

None

Command History

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

The following example shows how to configure an additional port number 1200 to be redirected for web authentication:

```
(Cisco Controller) > config network web-auth port 1200
```

Related Commands

show network summary

config network web-auth proxy-redirect

To configure proxy redirect support for web authentication clients, use the **config network web-auth proxy-redirect** command.

config network web-auth proxy-redirect {**enable** | **disable**}

Syntax Description

enable	Allows proxy redirect support for web authentication clients.
disable	Disallows proxy redirect support for web authentication clients.

Command Default

None

Command History

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

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands

show network summary

config network web-auth secureweb

To configure the secure web (https) authentication for clients, use the **config network web-auth secureweb** command.

config network web-auth secureweb {**enable** | **disable**}

Syntax Description

enable	Allows secure web (https) authentication for clients.
disable	Disallows secure web (https) authentication for clients. Enables http web authentication for clients.

Command Default

The default secure web (https) authentication for clients is enabled.

Command History

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

Usage Guidelines

If you configure the secure web (https) authentication for clients using the **config network web-auth secureweb disable** command, then you must reboot the Cisco WLC to implement the change.

The following example shows how to enable the secure web (https) authentication for clients:

```
(Cisco Controller) > config network web-auth secureweb enable
```

Related Commands

show network summary

config network web-auth https-redirect

To configure https redirect support for web authentication clients, use the **config network web-auth https-redirect** command.

config network web-auth https-redirect {**enable** | **disable**}

Syntax Description

enable	Enables the secure redirection(https) for web-authentication clients.
disable	Disables the secure redirection(https) for web-authentication clients.

Command Default

This command is by default disabled.

Command History

Release	Modification
8.0	This command was introduced in Release 8.0

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth https-redirect enable
```

Related Commands

show network summary

config network webmode

To enable or disable the web mode, use the **config network webmode** command.

config network webmode {**enable** | **disable**}

Syntax Description

enable	Enables the web interface.
disable	Disables the web interface.

Command Default

The default value for the web mode is **enable**.

Command History

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

The following example shows how to disable the web interface mode:

```
(Cisco Controller) > config network webmode disable
```

Related Commands

show network summary

config network web-auth

To configure the network-level web authentication options, use the **config network web-auth** command.

config network web-auth {**port** *port-number*} | {**proxy-redirect** {**enable** | **disable**}}

Syntax Description

port	Configures additional ports for web authentication redirection.
port-number	Port number (between 0 and 65535).
proxy-redirect	Configures proxy redirect support for web authentication clients.
enable	Enables proxy redirect support for web authentication clients. **Note** Web-auth proxy redirection will be enabled for ports 80, 8080, and 3128, along with user defined port 345.
disable	Disables proxy redirect support for web authentication clients.

Command Default

The default network-level web authentication value is disabled.

Command History

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

Usage Guidelines

You must reset the system for the configuration to take effect.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands

show network summary

show run-config

config qos protocol-type

config network zero-config

To configure bridge access point ZeroConfig support, use the **config network zero-config** command.

config network zero-config {**enable** | **disable**}

Syntax Description

enable	Enables the bridge access point ZeroConfig support.
disable	Disables the bridge access point ZeroConfig support.

Command Default

The bridge access point ZeroConfig support is enabled.

Command History

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

The following example shows how to enable the bridge access point ZeroConfig support:

```
(Cisco Controller) >config network zero-config enable
```

config nmsp notify-interval measurement

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **config nmsp notify-interval measurement** command.

config nmsp notify-interval measurement {**client** | **rfid** | **rogue**} *interval*

Syntax Description

client	Modifies the interval for clients.
rfid	Modifies the interval for active radio frequency identification (RFID) tags.
rogue	Modifies the interval for rogue access points and rogue clients.
interval	Time interval. The range is from 1 to 30 seconds.

Command Default

None

Command History

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

Usage Guidelines

The TCP port (16113) that the controller and location appliance communicate over must be open (not blocked) on any firewall that exists between the controller and the location appliance for NMSP to function.

The following example shows how to modify the NMSP notification interval for the active RFID tags to 25 seconds:

```
(Cisco Controller) > config nmsp notify-interval measurement rfid 25
```

Related Commands

clear locp statistics

clear nmsp statistics

show nmsp notify-interval summary

show nmsp statistics

show nmsp status

config paging

To enable or disable scrolling of the page, use the **config paging** command.

config paging {**enable** | **disable**}

Syntax Description

enable	Enables the scrolling of the page.
disable	Disables the scrolling of the page.

Command Default

By default, scrolling of the page is enabled.

Usage Guidelines

Commands that produce a huge number of lines of output with the scrolling of the page disabled might result in the termination of SSH/Telnet connection or user session on the console.

The following example shows how to enable scrolling of the page:

```
(Cisco Controller) > config paging enable
```

Related Commands

show run-config

config passwd-cleartext

To enable or disable temporary display of passwords in plain text, use the **config passwd-cleartext** command.

config passwd-cleartext {**enable** | **disable**}

Syntax Description

enable	Enables the display of passwords in plain text.
disable	Disables the display of passwords in plain text.

Command Default

By default, temporary display of passwords in plain text is disabled.

Command History

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

Usage Guidelines

This command must be enabled if you want to see user-assigned passwords displayed in clear text when using the **show run-config** command.

To execute this command, you must enter an admin password. This command is valid only for this particular session. It is not saved following a reboot.

The following example shows how to enable display of passwords in plain text:

```
(Cisco Controller) > config passwd-cleartext enable
The way you see your passwds will be changed
You are being warned.
Enter admin password:
```

Related Commands

show run-config

config prompt

To change the CLI system prompt, use the **config prompt** command.

config prompt *prompt*

Syntax Description

prompt	New CLI system prompt enclosed in double quotes. The prompt can be up to 31 alphanumeric characters and is case sensitive.

Command Default

The system prompt is configured using the startup wizard.

Command History

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

Usage Guidelines

Because the system prompt is a user-defined variable, it is omitted from the rest of this documentation.

The following example shows how to change the CLI system prompt to Cisco 4400:

```
(Cisco Controller) > config prompt "Cisco 4400"
```

config qos average-data-rate

To define the average data rate in Kbps for TCP traffic per user or per service set identifier (SSID), use the **config qos average-data-rate** command.

config qos average-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Syntax Description

bronze	Specifies the average data rate for the queue bronze.
silver	Specifies the average data rate for the queue silver.
gold	Specifies the average data rate for the queue gold.
platinum	Specifies the average data rate for the queue platinum.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
rate	Average data rate for TCP traffic per user. A value between 0 and 51,2000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None

Command History

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

The following example shows how to configure the average data rate 0 Kbps for the queue gold per SSID:

```
(Cisco Controller) > config qos average-data-rate gold per ssid downstream 0
```

Related Commands

config qos burst-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config wlan override-rate-limit

config qos average-realtime-rate

To define the average real-time data rate in Kbps for UDP traffic per user or per service set identifier (SSID), use the **config qos average-realtime-rate** command.

config qos average-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Syntax Description

bronze	Specifies the average real-time data rate for the queue bronze.
silver	Specifies the average real-time data rate for the queue silver.
gold	Specifies the average real-time data rate for the queue gold.
platinum	Specifies the average real-time data rate for the queue platinum.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
rate	Average real-time data rate for UDP traffic per user. A value between 0 and 51,2000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None

Command History

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

The following example shows how to configure the average real-time actual rate for queue gold:

```
(Cisco Controller) > config qos average-realtime-rate gold per ssid downstream 10
```

Related Commands

config qos average-data-rate

config qos burst-data-rate

config qos burst-realtime-rate

config wlan override-rate-limit

config qos burst-data-rate

To define the peak data rate in Kbps for TCP traffic per user or per service set identifier (SSID), use the **config qos burst-data-rate** command.

config qos burst-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Syntax Description

bronze	Specifies the peak data rate for the queue bronze.
silver	Specifies the peak data rate for the queue silver.
gold	Specifies the peak data rate for the queue gold.
platinum	Specifies the peak data rate for the queue platinum.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
rate	Peak data rate for TCP traffic per user. A value between 0 and 51,2000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None

Command History

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

The following example shows how to configure the peak rate 30000 Kbps for the queue gold:

```
(Cisco Controller) > config qos burst-data-rate gold per ssid downstream 30000
```

Related Commands

config qos average-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config wlan override-rate-limit

config qos burst-realtime-rate

To define the burst real-time data rate in Kbps for UDP traffic per user or per service set identifier (SSID), use the **config qos burst-realtime-rate** command.

config qos burst-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} { **per-ssid** | **per-client** } { **downstream** | **upstream** } *rate*

Syntax Description

bronze	Specifies the burst real-time data rate for the queue bronze.
silver	Specifies the burst real-time data rate for the queue silver.
gold	Specifies the burst real-time data rate for the queue gold.
platinum	Specifies the burst real-time data rate for the queue platinum.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
rate	Burst real-time data rate for UDP traffic per user. A value between 0 and 51,2000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None

Command History

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

The following example shows how to configure the burst real-time actual rate 2000 Kbps for the queue gold:

```
(Cisco Controller) > config qos burst-realtime-rate gold per ssid downstream  2000
```

Related Commands

config qos average-data-rate

config qos burst-data-rate

config qos average-realtime-rate

config wlan override-rate-limit

config qos description

To change the profile description, use the **config qos description** command.

config qos description {**bronze** | **silver** | **gold** | **platinum**} *description*

Syntax Description

bronze	Specifies the QoS profile description for the queue bronze.
silver	Specifies the QoS profile description for the queue silver.
gold	Specifies the QoS profile description for the queue gold.
platinum	Specifies the QoS profile description for the queue platinum.
description	QoS profile description.

Command Default

None

Command History

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

The following example shows how to configure the QoS profile description “description” for the queue gold:

```
(Cisco Controller) > config qos description gold abc
```

Related Commands

show qos average-data-rate

config qos burst-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config qos max-rf-usage

config qos max-rf-usage

To specify the maximum percentage of RF usage per access point, use the **config qos max-rf-usage** command.

config qos max-rf-usage {**bronze** | **silver** | **gold** | **platinum**} *usage_percentage*

Syntax Description

bronze	Specifies the maximum percentage of RF usage for the queue bronze.
silver	Specifies the maximum percentage of RF usage for the queue silver.
gold	Specifies the maximum percentage of RF usage for the queue gold.
platinum	Specifies the maximum percentage of RF usage for the queue platinum.
usage-percentage	Maximum percentage of RF usage.

Command Default

None

Command History

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

The following example shows how to specify the maximum percentage of RF usage for the queue gold:

```
(Cisco Controller) > config qos max-rf-usage gold 20
```

Related Commands

show qos description

config qos average-data-rate

config qos burst-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config qos dot1p-tag

To define the maximum value (0 to 7) for the priority tag associated with packets that fall within the profile, use the **config qos dot1p-tag** command.

config qos dot1p-tag {**bronze** | **silver** | **gold** | **platinum**} *dot1p_tag*

Syntax Description

bronze	Specifies the QoS 802.1p tag for the queue bronze.
silver	Specifies the QoS 802.1p tag for the queue silver.
gold	Specifies the QoS 802.1p tag for the queue gold.
platinum	Specifies the QoS 802.1p tag for the queue platinum.
dot1p_tag	Dot1p tag value between 1 and 7.

Command Default

None

Command History

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

The following example shows how to configure the a QoS 802.1p tag for the queue gold with the dot1p tag value of 5:

```
(Cisco Controller) > config qos dot1p-tag gold 5
```

Related Commands

show qos queue_length all

config qos protocol-type

config qos priority

To define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN, use the **config qos priority** command.

config qos priority {**bronze** | **silver** | **gold** | **platinum**} {*maximum-priority* | *default-unicast-priority* | *default-multicast-priority*}

Syntax Description

bronze	Specifies a Bronze profile of the WLAN.
silver	Specifies a Silver profile of the WLAN.
gold	Specifies a Gold profile of the WLAN.
platinum	Specifies a Platinum profile of the WLAN.
maximum-priority	Maximum QoS priority as one of the following: • besteffort • background • video • voice
default-unicast-priority	Default unicast priority as one of the following: • besteffort • background • video • voice
default-multicast-priority	Default multicast priority as one of the following: • besteffort • background • video • voice

Command History

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

Usage Guidelines

The maximum priority level should not be lower than the default unicast and multicast priority levels.

The following example shows how to configure the QoS priority for a gold profile of the WLAN with voice as the maximum priority, video as the default unicast priority, and besteffort as the default multicast priority.

```
(Cisco Controller) > config qos priority gold voice video besteffort
```

Related Commands **config qos protocol-type**

config qos protocol-type

To define the maximum value (0 to 7) for the priority tag associated with packets that fall within the profile, use the **config qos protocol-type** command.

config qos protocol-type {**bronze** | **silver** | **gold** | **platinum**} {**none** | *dot1p*}

Syntax Description

bronze	Specifies the QoS 802.1p tag for the queue bronze.
silver	Specifies the QoS 802.1p tag for the queue silver.
gold	Specifies the QoS 802.1p tag for the queue gold.
platinum	Specifies the QoS 802.1p tag for the queue platinum.
none	Specifies when no specific protocol is assigned.
dot1p	Specifies when dot1p type protocol is assigned.

Command Default

None

Command History

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

The following example shows how to configure the QoS protocol type silver:

```
(Cisco Controller) > config qos protocol-type silver dot1p
```

Related Commands

show qos queue_length all

config qos dot1p-tag

config qos queue_length

To specify the maximum number of packets that access points keep in their queues, use the **config qos queue_length** command.

config qos queue_length {**bronze** | **silver** | **gold** | **platinum**} *queue_length*

Syntax Description

bronze	Specifies the QoS length for the queue bronze.
silver	Specifies the QoS length for the queue silver.
gold	Specifies the QoS length for the queue gold.
platinum	Specifies the QoS length for the queue platinum.
queue_length	Maximum queue length values (10 to 255).

Command Default

None

Command History

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

The following example shows how to configure the QoS length for the queue “gold” with the maximum queue length value as 12:

```
(Cisco Controller) > config qos queue_length gold 12
```

Related Commands

show qos

config rfid auto-timeout

To configure an automatic timeout of radio frequency identification (RFID) tags, use the **config rfid auto-timeout** command.

config rfid auto-timeout {**enable** | **disable**}

Syntax Description

enable	Enables an automatic timeout.
disable	Disables an automatic timeout.

Command Default

None

Command History

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

The following example shows how to enable an automatic timeout of RFID tags:

```
(Cisco Controller) > config rfid auto-timeout enable
```

Related Commands

show rfid summary

config rfid status

config rfid timeout

config rfid status

To configure radio frequency identification (RFID) tag data tracking, use the **config rfid status** command.

config rfid status {**enable** | **disable**}

Syntax Description

enable	Enables RFID tag tracking.
disable	Enables RFID tag tracking.

Command Default

None

Command History

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

The following example shows how to configure RFID tag tracking settings:

```
(Cisco Controller) > config rfid status enable
```

Related Commands

show rfid summary

config rfid auto-timeout

config rfid timeout

config rfid timeout

To configure a static radio frequency identification (RFID) tag data timeout, use the **config rfid timeout** command.

config rfid timeout *seconds*

Syntax Description

seconds	Timeout in seconds (from 60 to 7200).

Command Default

None

Command History

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

The following example shows how to configure a static RFID tag data timeout of 60 seconds:

```
(Cisco Controller) > config rfid timeout 60
```

Related Commands

show rfid summary

config rfid statistics

config service timestamps

To enable or disable time stamps in message logs, use the **config service timestamps** command.

config service timestamps {**debug** | **log**} {**datetime** | **disable**}

Syntax Description

debug	Configures time stamps in debug messages.
log	Configures time stamps in log messages.
datetime	Specifies to time-stamp message logs with the standard date and time.
disable	Specifies to prevent message logs being time-stamped.

Command Default

By default, the time stamps in message logs are disabled.

Command History

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

The following example shows how to configure time-stamp message logs with the standard date and time:

```
(Cisco Controller) > config service timestamps log datetime
```

The following example shows how to prevent message logs being time-stamped:

```
(Cisco Controller) > config service timestamps debug disable
```

Related Commands

show logging

config sessions maxsessions

To configure the number of Telnet CLI sessions allowed by the Cisco wireless LAN controller, use the **config sessions maxsessions** command.

config sessions maxsessions *session_num*

Syntax Description

session_num	Number of sessions from 0 to 5.

Command Default

The default number of Telnet CLI sessions allowed by the Cisco WLC is 5.

Command History

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

Usage Guidelines

Up to five sessions are possible while a setting of zero prohibits any Telnet CLI sessions.

The following example shows how to configure the number of allowed CLI sessions to 2:

```
(Cisco Controller) > config sessions maxsessions 2
```

Related Commands

show sessions

config sessions timeout

To configure the inactivity timeout for Telnet CLI sessions, use the **config sessions timeout** command.

config sessions timeout *timeout*

Syntax Description

timeout	Timeout of Telnet session in minutes (from 0 to 160). A value of 0 indicates no timeout.

Command Default

The default inactivity timeout for Telnet CLI sessions is 5 minutes.

Command History

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

The following example shows how to configure the inactivity timeout for Telnet sessions to 20 minutes:

```
(Cisco Controller) > config sessions timeout 20
```

Related Commands

show sessions

config switchconfig boot-break

To enable or disable the breaking into boot prompt by pressing the Esc key at system startup, use the **config switchconfig boot-break** command.

config switchconfig boot-break {**enable** | **disable**}

Syntax Description

enable	Enables the breaking into boot prompt by pressing the Esc key at system startup.
disable	Disables the breaking into boot prompt by pressing the Esc key at system startup.

Command Default

By default, the breaking into boot prompt by pressing the Esc key at system startup is disabled.

Usage Guidelines

You must enable the features that are prerequisites for the Federal Information Processing Standard (FIPS) mode before enabling or disabling the breaking into boot prompt.

The following example shows how to enable the breaking into boot prompt by pressing the Esc key at system startup:

```
(Cisco Controller) > config switchconfig boot-break enable
```

Related Commands

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig fips-prerequisite

config switchconfig strong-pwd

config switchconfig fips-prerequisite

To enable or disable the features that are prerequisites for the Federal Information Processing Standard (FIPS) mode, use the **config switchconfig fips-prerequisite** command.

config switchconfig fips-prerequisite {**enable** | **disable**}

Syntax Description

enable	Enables the features that are prerequisites for the FIPS mode.
disable	Disables the features that are prerequisites for the FIPS mode.

Command Default

By default, the features that are prerequisites for the FIPS mode are disabled.

Usage Guidelines

You must configure the FIPS authorization secret before you can enable or disable the FIPS prerequisite features.

The following example shows how to enable the features that are prerequisites for the FIPS mode:

```
(Cisco Controller) > config switchconfig fips-prerequisite enable
```

Related Commands

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig boot-break

config switchconfig strong-pwd

config switchconfig strong-pwd

To enable or disable your controller to check the strength of newly created passwords, use the **config switchconfig strong-pwd** command.

config switchconfig strong-pwd {**case-check** | **consecutive-check** | **default-check** | **username-check** | **all-checks**} {**enable** | **disable**}

Syntax Description

case-check	Checks at least three combinations: lowercase characters, uppercase characters, digits, or special characters.
consecutive-check	Checks the occurrence of the same character three times.
default-check	Checks for default values or use of their variants.
username-check	Checks whether the username is specified or not.
all-checks	Checks all the cases.
enable	Enables a strong password check for the access point and Cisco WLC.
disable	Disables a strong password check for the access point and Cisco WLC.

Command Default

None

Command History

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

The following example shows how to enable the Strong Password Check feature:

```
(Cisco Controller) > config switchconfig strong-pwd case-check enable
```

Related Commands

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig fips-prerequisite

config switchconfig boot-break

config switchconfig flowcontrol

To enable or disable 802.3x flow control, use the **config switchconfig flowcontrol** command.

config switchconfig flowcontrol {**enable** | **disable**}

Syntax Description

enable	Enables 802.3x flow control.
disable	Disables 802.3x flow control.

Command Default

By default, 802.3x flow control is disabled.

The following example shows how to enable 802.3x flow control on Cisco wireless LAN controller parameters:

```
(Cisco Controller) > config switchconfig flowcontrol enable
```

Related Commands

show switchconfig

config switchconfig mode

To configure Lightweight Access Port Protocol (LWAPP) transport mode for Layer 2 or Layer 3, use the **config switchconfig mode** command.

config switchconfig mode {**L2** | **L3**}

Syntax Description

L2	Specifies Layer 2 as the transport mode.
L3	Specifies Layer 3 as the transport mode.

Command Default

The default transport mode is L3.

Command History

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

The following example shows how to configure LWAPP transport mode to Layer 3:

```
(Cisco Controller) > config switchconfig mode L3
```

Related Commands

show switchconfig

config switchconfig secret-obfuscation

To enable or disable secret obfuscation, use the **config switchconfig secret-obfuscation** command.

config switchconfig secret-obfuscation {**enable** | **disable**}

Syntax Description

enable	Enables secret obfuscation.
disable	Disables secret obfuscation.

Command Default

Secrets and user passwords are obfuscated in the exported XML configuration file.

Command History

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

Usage Guidelines

To keep the secret contents of your configuration file secure, do not disable secret obfuscation. To further enhance the security of the configuration file, enable configuration file encryption.

The following example shows how to enable secret obfuscation:

```
(Cisco Controller) > config switchconfig secret-obfuscation enable
```

Related Commands

show switchconfig

config sysname

To set the Cisco wireless LAN controller system name, use the **config sysname** command.

config sysname *name*

Syntax Description

name	System name. The name can contain up to 24 alphanumeric characters.

Command Default

None

Command History

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

The following example shows how to configure the system named Ent_01:

```
(Cisco Controller) > config sysname Ent_01
```

Related Commands

show sysinfo

config snmp community accessmode

To modify the access mode (read only or read/write) of an SNMP community, use the **config snmp community accessmode** command.

config snmp community accessmode {**ro** | **rw**} *name*

Syntax Description

ro	Specifies a read-only mode.
rw	Specifies a read/write mode.
name	SNMP community name.

Command Default

Two communities are provided by default with the following settings:

```
SNMP Community Name Client IP Address Client IP Mask   Access Mode Status
------------------- ----------------- ---------------- ----------- ------
public              0.0.0.0           0.0.0.0          Read Only   Enable
private             0.0.0.0           0.0.0.0          Read/Write  Enable
```

Command History

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

The following example shows how to configure read/write access mode for SNMP community:

```
(Cisco Controller) > config snmp community accessmode rw private
```

Related Commands

show snmp community

config snmp community mode

config snmp community create

config snmp community delete

config snmp community ipaddr

config snmp community create

To create a new SNMP community, use the **config snmp community create** command.

config snmp community create *name*

Syntax Description

name	SNMP community name of up to 16 characters.

Command Default

None

Command History

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

Usage Guidelines

Use this command to create a new community with the default configuration.

The following example shows how to create a new SNMP community named test:

```
(Cisco Controller) > config snmp community create test
```

Related Commands

show snmp community

config snmp community mode

config snmp community accessmode

config snmp community delete

config snmp community ipaddr

config snmp community delete

To delete an SNMP community, use the **config snmp community delete** command.

config snmp community delete *name*

Syntax Description

name	SNMP community name.

Command Default

None

Command History

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

The following example shows how to delete an SNMP community named test:

```
(Cisco Controller) > config snmp community delete test
```

Related Commands

show snmp community

config snmp community mode

config snmp community accessmode

config snmp community create

config snmp community ipaddr

config snmp community ipaddr

To configure the IPv4 or IPv6 address of an SNMP community, use the **config snmp community ipaddr** command.

config snmp community ipaddr *IP addr IPv4 mask/IPv6 Prefix lengthname*

Syntax Description

IP addr	SNMP community IPv4 or IPv6 address.
IPv4 mask/IPv6 Prefix length	SNMP community IP mask (IPv4 mask or IPv6 Prefix length). The IPv6 prefix length is from 0 to 128.
name	SNMP community name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

- This command is applicable for both IPv4 and IPv6 addresses.
- This command is not applicable for default SNMP community (public, private).

The following example shows how to configure an SNMP community with the IPv4 address 10.10.10.10, IPv4 mask 255.255.255.0, and SNMP community named comaccess:

```
(Cisco Controller) > config snmp community ipaddr 10.10.10.10 255.255.255.0 comaccess
```

The following example shows how to configure an SNMP community with the IPv6 address 2001:9:2:16::1, IPv6 prefix length 64, and SNMP community named comaccess:

```
(Cisco Controller) > config snmp community ipaddr 2001:9:2:16::1 64 comaccess
```

Related Topics

show snmpcommunity, on page 452
config snmp community accessmode, on page 283
config snmp community create, on page 284
config snmp community delete, on page 285
config snmp community mode, on page 287

config snmp community mode

To enable or disable an SNMP community, use the **config snmp community mode** command.

config snmp community mode {**enable** | **disable**} *name*

Syntax Description

enable	Enables the community.
disable	Disables the community.
name	SNMP community name.

Command Default

None

Command History

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

The following example shows how to enable the SNMP community named public:

```
(Cisco Controller) > config snmp community mode disable public
```

Related Commands

show snmp community

config snmp community delete

config snmp community accessmode

config snmp community create

config snmp community ipaddr

config snmp engineID

To configure the SNMP engine ID, use the **config snmp engineID** command.

config snmp engineID {*engine_id* | **default**}

Syntax Description

engine_id	Engine ID in hexadecimal characters (a minimum of 10 and a maximum of 24 characters are allowed).
default	Restores the default engine ID.

Command Default

None

Command History

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

Usage Guidelines

The SNMP engine ID is a unique string used to identify the device for administration purposes. You do need to specify an engine ID for the device because a default string is automatically generated using Cisco's enterprise number and the MAC address of the first interface on the device.

If you change the engine ID, then a reboot is required for the change to take effect.

Caution If you change the value of the SNMP engine ID, then the password of the user entered on the command line is converted to an MD5 (Message-Digest algorithm 5) or SHA (Secure Hash Algorithm) security digest. This digest is based on both the password and the local engine ID. The command line password is then deleted. Because of this deletion, if the local value of the engine ID changes, the security digests of the SNMP users will become invalid, and the users will have to be reconfigured.

The following example shows how to configure the SNMP engine ID with the value fffffffffff:

```
(Cisco Controller) > config snmp engineID fffffffffff
```

Related Commands

show snmpengineID

config snmp syscontact

To set the SNMP system contact name, use the **config snmp syscontact** command.

config snmp syscontact *contact*

Syntax Description

contact	SNMP system contact name. Valid value can be up to 255 printable characters.

Command Default

None

Command History

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

The following example shows how to set the SMNP system contact named Cisco WLAN Solution_administrator:

```
(Cisco Controller) > config snmp syscontact Cisco WLAN Solution_administrator
```

config snmp syslocation

To configure the SNMP system location name, use the **config snmp syslocation** command.

config snmp syslocation *location*

Syntax Description

location	SNMP system location name. Valid value can be up to 255 printable characters.

Command Default

None

Command History

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

The following example shows how to configure the SNMP system location name to Building_2a:

```
(Cisco Controller) > config snmp syslocation Building_2a
```

config snmp trapreceiver create

To configure a server to receive SNMP traps, use the **config snmp trapreceiver create** command.

config snmp trapreceiver create *name IP addr*

Syntax Description

name	SNMP community name. The name contain up to 31 characters.
IP addr	Configure the IPv4 or IPv6 address of where to send SNMP traps.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

The IPv4 or IPv6 address must be valid for the command to add the new server.

The following example shows how to add a new SNMP trap receiver with the SNMP trap receiver named test and IP address 10.1.1.1:

```
(Cisco Controller) > config snmp trapreceiver create test 10.1.1.1
```

The following example shows how to add a new SNMP trap receiver with the SNMP trap receiver named test and IP address 2001:10:1:1::1:

```
(Cisco Controller) > config snmp trapreceiver create test 2001:10:1:1::1
```

Related Topics

show snmptrap, on page 454

config snmp trapreceiver delete

To delete a server from the trap receiver list, use the **config snmp trapreceiver delete** command.

config snmp trapreceiver delete *name*

Syntax Description

name	SNMP community name. The name can contain up to 16 characters.

Command Default

None

Command History

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

The following example shows how to delete a server named test from the SNMP trap receiver list:

```
(Cisco Controller) > config snmp trapreceiver delete test
```

Related Commands

show snmp trap

config snmp trapreceiver mode

To send or disable sending traps to a selected server, use the **config snmp trapreceiver mode** command.

config snmp trapreceiver mode {**enable** | **disable**} *name*

Syntax Description

enable	Enables an SNMP trap receiver.
disable	Disables an SNMP trap receiver.
name	SNMP community name.

Command Default

None

Command History

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

Usage Guidelines

This command enables or disables the Cisco wireless LAN controller from sending the traps to the selected server.

The following example shows how to disable an SNMP trap receiver from sending traps to a server named server1:

```
(Cisco Controller) > config snmp trapreceiver mode disable server1
```

Related Commands

show snmp trap

config snmp v3user create

To create a version 3 SNMP user, use the **config snmp v3user create** command.

config snmp v3user create *username* {**ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des** | **aescfb128**} [*auth_key*] [*encrypt_key*]

Syntax Description

username	Version 3 SNMP username.
ro	Specifies a read-only user privilege.
rw	Specifies a read-write user privilege.
none	Specifies if no authentication is required.
hmacmd5	Specifies Hashed Message Authentication Coding Message Digest 5 (HMAC-MD5) for authentication.
hmacsha	Specifies Hashed Message Authentication Coding-Secure Hashing Algorithm (HMAC-SHA) for authentication.
none	Specifies if no encryption is required.
des	Specifies to use Cipher Block Chaining-Digital Encryption Standard (CBC-DES) encryption.
aescfb128	Specifies to use Cipher Feedback Mode-Advanced Encryption Standard-128 (CFB-AES-128) encryption.
auth_key	(Optional) Authentication key for the HMAC-MD5 or HMAC-SHA authentication protocol.
encrypt_key	(Optional) Encryption key for the CBC-DES or CFB-AES-128 encryption protocol.

Command Default

SNMP v3 username AccessMode Authentication Encryption

```
-------------------- ------------- -------------- -----------
default              Read/Write    HMAC-SHA       CFB-AES
```

Command History

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

The following example shows how to add an SNMP username named test with read-only privileges and no encryption or authentication:

```
(Cisco Controller) > config snmp v3user create test ro none none
```

Related Commands show snmpv3user

config snmp v3user delete

To delete a version 3 SNMP user, use the **config snmp v3user delete** command.

config snmp v3user delete *username*

Syntax Description

username	Username to delete.

Command Default

None

Command History

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

The following example shows how to remove an SNMP user named test:

```
(Cisco Controller) > config snmp v3user delete test
```

Related Commands

show snmp v3user

config snmp version

To enable or disable selected SNMP versions, use the **config snmp version** command.

config snmp version {**v1** | **v2** | **v3**} {**enable** | **disable**}

Syntax Description

v1	Specifies an SNMP version to enable or disable.
v2	Specifies an SNMP version to enable or disable.
v3	Specifies an SNMP version to enable or disable.
enable	Enables a specified version.
disable	Disables a specified version.

Command Default

By default, all the SNMP versions are enabled.

Command History

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

The following example shows how to enable SNMP version v1:

```
(Cisco Controller) > config snmp version v1 enable
```

Related Commands

show snmpversion

config time manual

To set the system time, use the **config time manual** command.

config time manual *MM* | *DD* | *YY HH*:*MM*:*SS*

Syntax Description

MM/*DD*/*YY*	Date.
HH:*MM*:*SS*	Time.

Command Default

None

Command History

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

The following example shows how to configure the system date to 04/04/2010 and time to 15:29:00:

```
(Cisco Controller) > config time manual 04/04/2010 15:29:00
```

Related Commands

show time

config time ntp

To set the Network Time Protocol (NTP), use the **config time ntp** command.

config time ntp {**auth** {**enable** *server-index key-index* | **disable** *server-index*} | **interval** *interval* | **key-auth** {**add** *key-index* **md5** {**ascii** | **hex**} *key*} | **delete** *key-index*} | **server** *index IP Address*}

Syntax Description

auth	Configures the NTP authentication.
enable	Enables the NTP authentication.
server-index	NTP server index.
key-index	Key index between 1 and 4294967295.
disable	Disables the NTP authentication.
interval	Configures the NTP version 3 polling interval.
interval	NTP polling interval in seconds. The range is from 3600 and 604800 seconds.
key-auth	Configures the NTP authentication key.
add	Adds an NTP authentication key.
md5	Specifies the authentication protocol.
ascii	Specifies the ASCII key type.
hex	Specifies the hexadecimal key type.
key	Specifies the ASCII key format with a maximum of 16 characters or the hexadecimal key format with a maximum of 32 digits.
delete	Deletes an NTP server.
server	Configures the NTP servers.
IP Address	NTP server's IP address. Use 0.0.0.0 or :: to delete entry.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

- To add the NTP server to the controller, use the **config time ntp server** *index IP Address* command.

- To delete the NTP server (IPv4) from the controller, use the **config time ntp server** *index 0.0.0.0* command.

  To delete the NTP server (IPv6) from the controller, use the **config time ntp server** *index ::* command.

- To display configured NTP server on the controller, use the **show time** command.

The following example shows how to configure the NTP polling interval to 7000 seconds:

```
(Cisco Controller) > config time ntp interval 7000
```

The following example shows how to enable NTP authentication where the server index is 4 and the key index is 1:

```
(Cisco Controller) > config time ntp auth enable 4 1
```

The following example shows how to add an NTP authentication key of value ff where the key format is in hexadecimal characters and the key index is 1:

```
(Cisco Controller) > config time ntp key-auth add 1 md5 hex ff
```

The following example shows how to add an NTP authentication key of value ff where the key format is in ASCII characters and the key index is 1:

```
(Cisco Controller) > config time ntp key-auth add 1 md5 ascii ciscokey
```

The following example shows how to add NTP servers and display the servers configured to controllers:

```
(Cisco Controller) > config time ntp server  1 10.92.125.52
(Cisco Controller) > config time ntp server  2 2001:9:6:40::623
(Cisco Controller) > show time
Time..................................... Fri May 23 12:04:18 2014

Timezone delta.................................. 0:0
Timezone location.............................. (GMT +5:30) Colombo, New Delhi, Chennai,
 Kolkata

NTP Servers
NTP Polling Interval........................ 3600

Index NTP Key Index  NTP Server NTP    Msg Auth Status
------- ------------------------------------------------
1            1      10.92.125.52       AUTH SUCCESS
2            1      2001:9:6:40::623   AUTH SUCCESS
```

The following example shows how to delete NTP servers and verify that the servers are deleted removed from the NTP server list:

```
(Cisco Controller) > config time ntp server  1 0.0.0.0
(Cisco Controller) > config time ntp server  2 ::
(Cisco Controller) > show time
Time..................................... Fri May 23 12:04:18 2014
```

```
Timezone delta.................................. 0:0
Timezone location.............................. (GMT +5:30) Colombo, New Delhi, Chennai,
 Kolkata

NTP Servers
NTP Polling Interval........................ 3600

Index NTP Key Index  NTP Server NTP    Msg Auth Status
------- ------------------------------------------------
```

Related Topics

show time, on page 461
show ntp-keys, on page 446

config time timezone

To configure the system time zone, use the **config time timezone** command.

config time timezone {**enable** | **disable**} *delta_hours delta_mins*

Syntax Description

enable	Enables daylight saving time.
disable	Disables daylight saving time.
delta_hours	Local hour difference from the Universal Coordinated Time (UCT).
delta_mins	Local minute difference from UCT.

Command Default

None

Command History

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

The following example shows how to enable the daylight saving time:

```
(Cisco Controller) > config time timezone enable 2 0
```

Related Commands

show time

config time timezone location

To set the location of the time zone in order to have daylight saving time set automatically when it occurs, use the **config time timezone location** command.

config time timezone location *location_index*

Syntax Description *location_index*

Number representing the time zone required. The time zones are as follows:

- (GMT-12:00) International Date Line West
- (GMT-11:00) Samoa
- (GMT-10:00) Hawaii
- (GMT-9:00) Alaska
- (GMT-8:00) Pacific Time (US and Canada)
- (GMT-7:00) Mountain Time (US and Canada)
- (GMT-6:00) Central Time (US and Canada)
- (GMT-5:00) Eastern Time (US and Canada)
- (GMT-4:00) Atlantic Time (Canada)
- (GMT-3:00) Buenos Aires (Argentina)
- (GMT-2:00) Mid-Atlantic
- (GMT-1:00) Azores
- (GMT) London, Lisbon, Dublin, Edinburgh (default value)
- (GMT +1:00) Amsterdam, Berlin, Rome, Vienna
- (GMT +2:00) Jerusalem
- (GMT +3:00) Baghdad
- (GMT +4:00) Muscat, Abu Dhabi
- (GMT +4:30) Kabul
- (GMT +5:00) Karachi, Islamabad, Tashkent
- (GMT +5:30) Colombo, Kolkata, Mumbai, New Delhi
- (GMT +5:45) Katmandu
- (GMT +6:00) Almaty, Novosibirsk
- (GMT +6:30) Rangoon
- (GMT +7:00) Saigon, Hanoi, Bangkok, Jakatar
- (GMT +8:00) Hong Kong, Bejing, Chongquing
- (GMT +9:00) Tokyo, Osaka, Sapporo
- (GMT +9:30) Darwin
- (GMT+10:00) Sydney, Melbourne, Canberra
- (GMT+11:00) Magadan, Solomon Is., New

Caledonia

- (GMT+12:00) Kamchatka, Marshall Is., Fiji
- (GMT+12:00) Auckland (New Zealand)

Command Default None

Command History

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

The following example shows how to set the location of the time zone in order to set the daylight saving time to location index 10 automatically:

```
(Cisco Controller) > config time timezone location 10
```

Related Commands **show time**

config trapflags 802.11-Security

To enable or disable sending 802.11 security-related traps, use the **config trapflags 802.11-Security** command.

config trapflags 802.11-Security wepDecryptError {**enable** | **disable**}

Syntax Description

enable	Enables sending 802.11 security-related traps.
disable	Disables sending 802.11 security-related traps.

Command Default

By default, sending the 802.11 security-related traps is enabled.

Command History

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

The following example shows how to disable the 802.11 security related traps:

```
(Cisco Controller) > config trapflags 802.11-Security wepDecryptError disable
```

Related Commands

show trapflags

config trapflags aaa

To enable or disable the sending of AAA server-related traps, use the **config trapflags aaa** command.

config trapflags aaa {**auth** | **servers**} {**enable** | **disable**}

Syntax Description

auth	Enables trap sending when an AAA authentication failure occurs for management user, net user, or MAC filter.
servers	Enables trap sending when no RADIUS servers are responding.
enable	Enables the sending of AAA server-related traps.
disable	Disables the sending of AAA server-related traps.

Command Default

By default, the sending of AAA server-related traps is enabled.

Command History

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

The following example shows how to enable the sending of AAA server-related traps:

```
(Cisco Controller) > config trapflags aaa auth enable
```

Related Commands

show watchlist

config trapflags adjchannel-rogueap

To configure trap notifications when a rogue access point is detected at the adjacent channel, use the **config trapflags adjchannel-rogueap** command.

config trapflags adjchannel-rogueap {**enable** | **disable**}

Syntax Description

enable	Enables trap notifications when a rogue access point is detected at the adjacent channel.
disable	Disables trap notifications when a rogue access point is detected at the adjacent channel.

Command Default

None

Command History

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

The following example shows how to enable trap notifications when a rogue access point is detected at the adjacent channel:

```
(Cisco Controller) > config trapflags adjchannel-rogueap enable
```

Related Commands

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags mesh

config trapflags strong-pwdcheck

config trapflags rfid

config trapflags rogueap

show trapflags

config trapflags ap

To enable or disable the sending of Cisco lightweight access point traps, use the **config trapflags ap** command.

config trapflags ap {**register** | **interfaceUp**} {**enable** | **disable**}

Syntax Description

register	Enables sending a trap when a Cisco lightweight access point registers with Cisco switch.
interfaceUp	Enables sending a trap when a Cisco lightweight access point interface (A or B) comes up.
enable	Enables sending access point-related traps.
disable	Disables sending access point-related traps.

Command Default

By default, the sending of Cisco lightweight access point traps is enabled.

Command History

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

The following example shows how to prevent traps from sending access point-related traps:

```
(Cisco Controller) > config trapflags ap register disable
```

Related Commands

show trapflags

config trapflags authentication

To enable or disable sending traps with invalid SNMP access, use the **config trapflags authentication** command.

config trapflags authentication {**enable** | **disable**}

Syntax Description

enable	Enables sending traps with invalid SNMP access.
disable	Disables sending traps with invalid SNMP access.

Command Default

By default, the sending traps with invalid SNMP access is enabled.

Command History

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

The following example shows how to prevent sending traps on invalid SNMP access:

```
(Cisco Controller) > config trapflags authentication disable
```

Related Commands

show trapflags

config trapflags client

To enable or disable the sending of client-related DOT11 traps, use the **config trapflags client** command.

config trapflags client {**802.11-associate 802.11-disassociate** | **802.11-deauthenticate** | **802.11-authfail** | **802.11-assocfail** | **authentication** | **excluded**} {**enable** | **disable**}

Syntax Description

802.11-associate	Enables the sending of Dot11 association traps to clients.
802.11-disassociate	Enables the sending of Dot11 disassociation traps to clients.
802.11-deauthenticate	Enables the sending of Dot11 deauthentication traps to clients.
802.11-authfail	Enables the sending of Dot11 authentication fail traps to clients.
802.11-assocfail	Enables the sending of Dot11 association fail traps to clients.
authentication	Enables the sending of authentication success traps to clients.
excluded	Enables the sending of excluded trap to clients.
enable	Enables sending of client-related DOT11 traps.
disable	Disables sending of client-related DOT11 traps.

Command Default

By default, the sending of client-related DOT11 traps is disabled.

Command History

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

The following example shows how to enable the sending of Dot11 disassociation trap to clients:

```
(Cisco Controller) > config trapflags client 802.11-disassociate enable
```

Related Commands

show trapflags

config trapflags client max-warning-threshold

To configure the threshold value of the number of clients that associate with the controller, after which an SNMP trap and a syslog message is sent to the controller, use the **config trapflags client max-warning-threshold** command.

config trapflags client max-warning-threshold {**threshold** | **enable** | **disable**}

Syntax Description

threshold	Configures the threshold percentage value of the number of clients that associate with the controller, after which an SNMP trap and a syslog message is sent to the controller. The range is from 80 to 100. The minimum interval between two warnings is 10 mins You cannot configure this interval.
enable	Enables the generation of the traps and syslog messages.
disable	Disables the generation of the traps and syslog messages.

Command Default

The default threshold value of the number of clients that associate with the controller is 90 %.

Command History

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

Usage Guidelines

This table lists the maximum number of clients for different controllers.

Table 1: Maximum Number of Clients Supported on Different Controllers

Controller	Maximum Number of Supported Clients
Cisco 5500 Series Controllers	7000
Cisco 2500 Series Controllers	500
Cisco Wireless Services Module 2	15000
Cisco Flex 7500 Series Controllers	64000
Cisco 8500 Series Controllers	64000
Cisco Virtual Wireless LAN Controllers	30000

The following example shows how to configure the threshold value of the number of clients that associate with the controller:

```
(Cisco Controller) > config trapflags client max-warning-threshold 80
```

Related Commands

show trapflags

config trapflags client

config trapflags configsave

To enable or disable the sending of configuration-saved traps, use the **config trapflags configsave** command.

config trapflags configsave {**enable** | **disable**}

Syntax Description

enable	Enables sending of configuration-saved traps.
disable	Disables the sending of configuration-saved traps.

Command Default

By default, the sending of configuration-saved traps is enabled.

Command History

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

The following example shows how to enable the sending of configuration-saved traps:

```
(Cisco Controller) > config trapflags configsave enable
```

Related Commands

show trapflags

config trapflags IPsec

To enable or disable the sending of IPsec traps, use the **config trapflags IPsec** command.

config trapflags IPsec {**esp-auth** | **esp-reply** | **invalidSPI** | **ike-neg** | **suite-neg** | **invalid-cookie**} {**enable** | **disable**}

Syntax Description

esp-auth	Enables the sending of IPsec traps when an ESP authentication failure occurs.
esp-reply	Enables the sending of IPsec traps when an ESP replay failure occurs.
invalidSPI	Enables the sending of IPsec traps when an ESP invalid SPI is detected.
ike-neg	Enables the sending of IPsec traps when an IKE negotiation failure occurs.
suite-neg	Enables the sending of IPsec traps when a suite negotiation failure occurs.
invalid-cookie	Enables the sending of IPsec traps when a Isakamp invalid cookie is detected.
enable	Enables sending of IPsec traps.
disable	Disables sending of IPsec traps.

Command Default

By default, the sending of IPsec traps is enabled.

Command History

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

The following example shows how to enable the sending of IPsec traps when ESP authentication failure occurs:

```
(Cisco Controller) > config trapflags IPsec esp-auth enable
```

Related Commands

show trapflags

config trapflags linkmode

To enable or disable Cisco wireless LAN controller level link up/down trap flags, use the **config trapflags linkmode** command.

config trapflags linkmode {**enable** | **disable**}

Syntax Description

enable	Enables Cisco wireless LAN controller level link up/down trap flags.
disable	Disables Cisco wireless LAN controller level link up/down trap flags.

Command Default

By default, the Cisco WLC level link up/down trap flags are enabled.

Command History

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

The following example shows how to enable the Cisco wireless LAN controller level link up/down trap:

```
(Cisco Controller) > config trapflags linkmode disable
```

Related Commands

show trapflags

config trapflags mesh

To configure trap notifications when a mesh access point is detected, use the **config trapflags mesh** command.

config trapflags mesh {**enable** | **disable**}

Syntax Description

enable	Enables trap notifications when a mesh access point is detected.
disable	Disables trap notifications when a mesh access point is detected.

Command Default

None

Command History

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

The following example shows how to enable trap notifications when a mesh access point is detected:

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

Related Commands

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags adjchannel-rogueap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags strong-pwdcheck

config trapflags rfid

config trapflags rogueap

show trapflags

config trapflags multiusers

To enable or disable the sending of traps when multiple logins are active, use the **config trapflags multiusers** command.

config trapflags multiusers {**enable** | **disable**}

Syntax Description

enable	Enables the sending of traps when multiple logins are active.
disable	Disables the sending of traps when multiple logins are active.

Command Default

By default, the sending of traps when multiple logins are active is enabled.

Command History

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

The following example shows how to disable the sending of traps when multiple logins are active:

```
(Cisco Controller) > config trapflags multiusers disable
```

Related Commands

show trapflags

config trapflags rfid

To configure the threshold value of the maximum number of radio frequency identification (RFID) tags, after which an SNMP trap and a syslog message is sent to the controller, use the **config trapflags rfid** command.

config trapflags rfid {**threshold** | **enable** | **disable**}

Syntax Description

threshold	Configures the threshold percentage value of the maximum number of RFID tags, after which an SNMP trap and a syslog message is sent to the controller. The range is from 80 to 100. The traps and syslog messages are generated every 10 minutes. You cannot configure this interval.
enable	Enables the generation of the traps and syslog messages.
disable	Disables the generation of the traps and syslog messages.

Command Default

The default threshold value of the maximum number of RFID tags is 90 %.

Command History

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

Usage Guidelines

The following table shows the maximum number of RFID tags supported on different controllers:

Table 2: Maximum Number of RFID Tags Supported on Different Controllers

Controller	Maximum Number of Supported Clients
Cisco 5500 Series Controllers	5000
Cisco 2500 Series Controllers	500
Cisco Wireless Services Module 2	10000
Cisco Flex 7500 Series Controllers	50000
Cisco 8500 Series Controllers	50000
Cisco Virtual Wireless LAN Controllers	3000

The following example shows how to configure the threshold value of the maximum number of RFID tags:

```
(Cisco Controller) > config trapflags rfid 80
```

Related Commands

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags adjchannel-rogueap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags mesh

config trapflags strong-pwdcheck

config trapflags rogueap

config trapflags mesh

show trapflags

config trapflags rogueap

To enable or disable sending rogue access point detection traps, use the **config trapflags rogueap** command.

config trapflags rogueap {**enable** | **disable**}

Syntax Description

enable	Enables the sending of rogue access point detection traps.
disable	Disables the sending of rogue access point detection traps.

Command Default

By default, the sending of rogue access point detection traps is enabled.

Command History

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

The following example shows how to disable the sending of rogue access point detection traps:

```
(Cisco Controller) > config trapflags rogueap disable
```

Related Commands

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue ap timeout

config rogue ap valid-client

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show trapflags

config trapflags rrm-params

To enable or disable the sending of Radio Resource Management (RRM) parameters traps, use the **config trapflags rrm-params** command.

config trapflags rrm-params {**tx-power** | **channel** | **antenna**} {**enable** | **disable**}

Syntax Description

tx-power	Enables trap sending when the RF manager automatically changes the tx-power level for the Cisco lightweight access point interface.
channel	Enables trap sending when the RF manager automatically changes the channel for the Cisco lightweight access point interface.
antenna	Enables trap sending when the RF manager automatically changes the antenna for the Cisco lightweight access point interface.
enable	Enables the sending of RRM parameter-related traps.
disable	Disables the sending of RRM parameter-related traps.

Command Default

By default, the sending of RRM parameters traps is enabled.

Command History

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

The following example shows how to enable the sending of RRM parameter-related traps:

```
(Cisco Controller) > config trapflags rrm-params tx-power enable
```

Related Commands

show trapflags

config trapflags rrm-profile

To enable or disable the sending of Radio Resource Management (RRM) profile-related traps, use the **config trapflags rrm-profile** command.

config trapflags rrm-profile {**load** | **noise** | **interference** | **coverage**} {**enable** | **disable**}

Syntax Description

load	Enables trap sending when the load profile maintained by the RF manager fails.
noise	Enables trap sending when the noise profile maintained by the RF manager fails.
interference	Enables trap sending when the interference profile maintained by the RF manager fails.
coverage	Enables trap sending when the coverage profile maintained by the RF manager fails.
enable	Enables the sending of RRM profile-related traps.
disable	Disables the sending of RRM profile-related traps.

Command Default

By default, the sending of RRM profile-related traps is enabled.

Command History

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

The following example shows how to disable the sending of RRM profile-related traps:

```
(Cisco Controller) > config trapflags rrm-profile load disable
```

Related Commands

show trapflags

config trapflags stpmode

To enable or disable the sending of spanning tree traps, use the **config trapflags stpmode** command.

config trapflags stpmode {**enable** | **disable**}

Syntax Description

enable	Enables the sending of spanning tree traps.
disable	Disables the sending of spanning tree traps.

Command Default

By default, the sending of spanning tree traps is enabled.

Command History

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

The following example shows how to disable the sending of spanning tree traps:

```
(Cisco Controller) > config trapflags stpmode disable
```

Related Commands

show trapflags

config trapflags strong-pwdcheck

To configure trap notifications for strong password checks, use the **config trapflags strong-pwdcheck** command.

config trapflags strong-pwdcheck {**enable** | **disable**}

Syntax Description

enable	Enables trap notifications for strong password checks.
disable	Disables trap notifications for strong password checks.

Command Default

None

Command History

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

The following example shows how to enable trap notifications for strong password checks:

```
(Cisco Controller) > config trapflags strong-pwdcheck enable
```

Related Commands

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags adjchannel-rogueap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags mesh

config trapflags rfid

config trapflags rogueap

show trapflags

config trapflags wps

To enable or disable Wireless Protection System (WPS) trap sending, use the **config trapflags wps** command.

config trapflags wps {**enable** | **disable**}

Syntax Description

enable	Enables WPS trap sending.
disable	Disables WPS trap sending.

Command Default

By default, the WPS trap sending is enabled.

Command History

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

The following example shows how to disable the WPS traps sending:

```
(Cisco Controller) > config trapflags wps disable
```

Related Commands

show trapflags

Timeout Commands

config 802.11 cac video tspec-inactivity-timeout

To process or ignore the Call Admission Control (CAC) Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point, use the **config 802.11 cac video tspec-inactivity-timeout** command.

config 802.11 {**a** | **b**} **cac video tspec-inactivity-timeout** {**enable** | **ignore**}

Syntax Description

a	Specifies the 802.11a network.
ab	Specifies the 802.11b/g network.
enable	Processes the TSPEC inactivity timeout messages.
ignore	Ignores the TSPEC inactivity timeout messages.

Command Default

The default CAC WMM TSPEC inactivity timeout received from an access point is disabled (ignore).

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

This example shows how to process the response to TSPEC inactivity timeout messages received from an access point:

```
(Cisco Controller) > config 802.11a cac video tspec-inactivity-timeout enable
```

This example shows how to ignore the response to TSPEC inactivity timeout messages received from an access point:

```
(Cisco Controller) > config 802.11a cac video tspec-inactivity-timeout ignore
```

Related Commands

config 802.11 cac video acm

config 802.11 cac video max-bandwidth

config 802.11 cac video roam-bandwidth

config 802.11 cac voice tspec-inactivity-timeout

To process or ignore the Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point, use the **config 802.11 cac voice tspec-inactivity-timeout** command.

config 802.11 {**a** | **b**} **cac voice tspec-inactivity-timeout** {**enable** | **ignore**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Processes the TSPEC inactivity timeout messages.
ignore	Ignores the TSPEC inactivity timeout messages.

Command Default

The default WMM TSPEC inactivity timeout received from an access point is disabled (ignore).

Usage Guidelines

Call Admission Control (CAC) commands require that the WLAN you are planning to modify is configured for Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

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

The following example shows how to enable the voice TSPEC inactivity timeout messages received from an access point:

```
(Cisco Controller) > config 802.11 cac voice tspec-inactivity-timeout enable
```

Related Commands

config 802.11 cac voice load-based

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice acm

config 802.11cac voice max-bandwidth

config 802.11 cac voice stream-size

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.
seconds	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.
discovery-timeout	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.
fast_heartbeat_seconds	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.

heartbeat_seconds	Cisco 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.
primary_discovery_timeout	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.
primed_join_timeout	Access point primed discovery timeout value, in seconds. The range is from 120 to 43200.
auth-timeout	Configures the authentication timeout.
auth_timeout	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.
watchdog_timer	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.
eap_identity_request_delay	Advanced EAP identity request delay, in seconds. The range is from 0 to 10.
eap-timeout	Configures the EAP expiration timeout.
eap_timeout	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
7.6	This command was introduced in a release earlier than Release 7.6.
8.3	This command was enhanced.

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 dhcp timeout

To configure a DHCP timeout value, use the **config dhcp timeout** command. If you have configured a WLAN to be in DHCP required state, this timer controls how long the WLC will wait for a client to get a DHCP lease through DHCP.

config dhcp timeout *timeout-value*

Syntax Description

timeout-value	Timeout value in the range of 5 to 120 seconds.

Command Default

The default timeout value is 120 seconds.

Command History

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

The following example shows how to set the DHCP timeout to 10 seconds:

```
(Cisco Controller) >config dhcp timeout 10
```

config ldap

To configure the Lightweight Directory Access Protocol (LDAP) server settings, use the **config ldap** command.

config ldap {**add** | **delete** | **enable** | **disable** | **retransmit-timeout** | **retry** | **user** | **simple-bind**} *index*

config ldap add *index server_ip_address port user_base user_attr user_type* [ ]

config ldap retransmit-timeout *index retransmit-timeout*

config ldap retry *attempts*

config ldap user {**attr** *index user-attr* | **base** *index user-base* | **type***index user-type*}

config ldap simple-bind {**anonymous** *index* | **authenticated** *index username password*}

Syntax Description

add	Specifies that an LDAP server is being added.
delete	Specifies that an LDAP server is being deleted.
enable	Specifies that an LDAP serve is enabled.
disable	Specifies that an LDAP server is disabled.
retransmit-timeout	Changes the default retransmit timeout for an LDAP server.
retry	Configures the retry attempts for an LDAP server.
user	Configures the user search parameters.
simple-bind	Configures the local authentication bind method.
anonymous	Allows anonymous access to the LDAP server.
authenticated	Specifies that a username and password be entered to secure access to the LDAP server.
index	LDAP server index. The range is from 1 to 17.
server_ip_address	IP address of the LDAP server.
port	Port number.
user_base	Distinguished name for the subtree that contains all of the users.
user_attr	Attribute that contains the username.
user_type	ObjectType that identifies the user.
retransmit-timeout	Retransmit timeout for an LDAP server. The range is from 2 to 30.

attempts	Number of attempts that each LDAP server is retried.
attr	Configures the attribute that contains the username.
base	Configures the distinguished name of the subtree that contains all the users.
type	Configures the user type.
username	Username for the authenticated bind method.
password	Password for the authenticated bind method.

Command Default None

Command History

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

The following example shows how to enable LDAP server index 10:

```
(Cisco Controller) > config ldap enable 10
```

Related Commands

config ldap add

config ldap simple-bind

show ldap summary

config remote-lan session-timeout

To configure client session timeout, use the **config remote-lan session-timeout** command.

config remote-lan session-timeout *remote-lan-id seconds*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
seconds	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

Command Default None

Command History

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

The following example shows how to configure the client session timeout to 6000 seconds for a remote LAN with ID 1:

```
(Cisco Controller) >config remote-lan session-timeout 1 6000
```

config network usertimeout

To change the timeout for idle client sessions, use the **config network usertimeout** command.

config network usertimeout *seconds*

Syntax Description

seconds	Timeout duration in seconds. The minimum value is 90 seconds. The default value is 300 seconds.

Command Default

The default timeout value for idle client session is 300 seconds.

Usage Guidelines

Use this command to set the idle client session duration on the Cisco wireless LAN controller. The minimum duration is 90 seconds.

The following example shows how to configure the idle session timeout to 1200 seconds:

```
(Cisco Controller) > config network usertimeout 1200
```

Related Commands

show network summary

config radius acct retransmit-timeout

To change the default transmission timeout for a RADIUS accounting server for the Cisco wireless LAN controller, use the **config radius acct retransmit-timeout** command.

config radius acct retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None

Command History

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

The following example shows how to configure retransmission timeout value 5 seconds between the retransmission:

```
(Cisco Controller) > config radius acct retransmit-timeout 5
```

Related Commands

show radius acct statistics

config radius auth mgmt-retransmit-timeout

To configure a default RADIUS server retransmission timeout for management users, use the **config radius auth mgmt-retransmit-timeout** command.

config radius auth mgmt-retransmit-timeout *index retransmit-timeout*

Syntax Description

index	RADIUS server index.
retransmit-timeout	Timeout value. The range is from 1 to 30 seconds.

Command Default

None

Command History

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

The following example shows how to configure a default RADIUS server retransmission timeout for management users:

```
(Cisco Controller) > config radius auth mgmt-retransmit-timeout 1 10
```

Related Commands

config radius auth management

config radius auth retransmit-timeout

To change a default transmission timeout for a RADIUS authentication server for the Cisco wireless LAN controller, use the **config radius auth retransmit-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None

Command History

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

The following example shows how to configure a retransmission timeout of 5 seconds for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth retransmit-timeout 5
```

Related Commands **show radius auth statistics**

config radius auth retransmit-timeout

To configure a retransmission timeout value for a RADIUS accounting server, use the **config radius auth server-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Timeout value. The range is from 2 to 30 seconds.

Command Default The default timeout is 2 seconds.

Command History

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

The following example shows how to configure a server timeout value of 2 seconds for RADIUS authentication server index 10:

```
(Cisco Controller) > config radius auth retransmit-timeout 2 10
```

Related Commands **show radius auth statistics**

show radius summary

config rogue ap timeout

To specify the number of seconds after which the rogue access point and client entries expire and are removed from the list, use the **config rogue ap timeout** command.

config rogue ap timeout *seconds*

Syntax Description

seconds	Value of 240 to 3600 seconds (inclusive), with a default value of 1200 seconds.

Command Default The default number of seconds after which the rogue access point and client entries expire is 1200 seconds.

Command History

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

The following example shows how to set an expiration time for entries in the rogue access point and client list to 2400 seconds:

```
(Cisco Controller) > config rogue ap timeout 2400
```

Related Commands

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config tacacs athr mgmt-server-timeout

To configure a default TACACS+ authorization server timeout for management users, use the **config tacacs athr mgmt-server-timeout** command.

config tacacs athr mgmt-server-timeout *index timeout*

Syntax Description

index	TACACS+ authorization server index.
timeout	Timeout value. The range is 1 to 30 seconds.

Command Default

None

Command History

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

The following example shows how to configure a default TACACS+ authorization server timeout for management users:

```
(Cisco Controller) > config tacacs athr mgmt-server-timeout 1 10
```

config tacacs auth mgmt-server-timeout

To configure a default TACACS+ authentication server timeout for management users, use the **config tacacs auth mgmt-server-timeout** command.

config tacacs auth mgmt-server-timeout *index timeout*

Syntax Description

index	TACACS+ authentication server index.
timeout	Timeout value. The range is 1 to 30 seconds.

Command Default None

Command History

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

The following example shows how to configure a default TACACS+ authentication server timeout for management users:

```
(Cisco Controller) > config tacacs auth mgmt-server-timeout 1 10
```

Related Commands **config tacacs auth**

config rfid auto-timeout

To configure an automatic timeout of radio frequency identification (RFID) tags, use the **config rfid auto-timeout** command.

config rfid auto-timeout {**enable** | **disable**}

Syntax Description

enable	Enables an automatic timeout.
disable	Disables an automatic timeout.

Command Default None

Command History

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

The following example shows how to enable an automatic timeout of RFID tags:

```
(Cisco Controller) > config rfid auto-timeout enable
```

Related Commands **show rfid summary**

config rfid status

config rfid timeout

config rfid timeout

To configure a static radio frequency identification (RFID) tag data timeout, use the **config rfid timeout** command.

config rfid timeout *seconds*

Syntax Description

seconds	Timeout in seconds (from 60 to 7200).

Command Default

None

Command History

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

The following example shows how to configure a static RFID tag data timeout of 60 seconds:

```
(Cisco Controller) > config rfid timeout 60
```

Related Commands

show rfid summary

config rfid statistics

config wlan session-timeout

To change the timeout of wireless LAN clients, use the **config wlan session-timeout** command.

config wlan session-timeout {*wlan_id* | **foreignAp**} *seconds*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

seconds	Timeout or session duration in seconds. A value of zero is equivalent to no timeout. **Note** The range of session timeout depends on the security type: • Open system: 0-65535 (sec) • 802.1x: 300-86400 (sec) • static wep: 0-65535 (sec) • cranite: 0-65535 (sec) • fortress: 0-65535 (sec) • CKIP: 0-65535 (sec) • open+web auth: 0-65535 (sec) • web pass-thru: 0-65535 (sec) • wpa-psk: 0-65535 (sec) • disable: To disable reauth/session-timeout timers.

Command Default

None

Usage Guidelines

For 802.1X client security type, which creates the PMK cache, the maximum session timeout that can be set is 86400 seconds when the session timeout is disabled. For other client security such as open, WebAuth, and PSK for which the PMK cache is not created, the session timeout value is shown as infinite when session timeout is disabled.

Command History

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

The following example shows how to configure the client timeout to 6000 seconds for WLAN ID 1:

```
(Cisco Controller) >config wlan session-timeout 1 6000
```

config wlan usertimeout

To configure the timeout for idle client sessions for a WLAN, use the **config wlan usertimeout** command.

config wlan usertimeout *timeout wlan_id*

Syntax Description

timeout	Timeout for idle client sessions for a WLAN. If the client sends traffic less than the threshold, the client is removed on timeout. The range is from 15 to 100000 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The default client session idle timeout is 300 seconds.

Command History

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

Usage Guidelines

The timeout value that you configure here overrides the global timeout that you define using the command **config network usertimeout**.

The following example shows how to configure the idle client sessions for a WLAN:

```
(Cisco Controller) >config wlan usertimeout 100 1
```

config wlan security wpa akm ft

To configure authentication key-management using 802.11r fast transition 802.1X, use the **config wlan security wpa akm ft** command.

config wlan security wpa akm ft [**over-the-air** | **over-the-ds** | **psk** | [**reassociation-timeout** *seconds*]] {**enable** | **disable**} *wlan_id*

Syntax Description

over-the-air	(Optional) Configures 802.11r fast transition roaming over-the-air support.
over-the-ds	(Optional) Configures 802.11r fast transition roaming DS support.
psk	(Optional) Configures 802.11r fast transition PSK support.
reassociation-timeout	(Optional) Configures the reassociation deadline interval. The valid range is between 1 to 100 seconds. The default value is 20 seconds.
seconds	Reassociation deadline interval in seconds.
enable	Enables 802.11r fast transition 802.1X support.
disable	Disables 802.11r fast transition 802.1X support.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

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

The following example shows how to configure authentication key-management using 802.11r fast transition:

```
(Cisco Controller) >config wlan security wpa akm ft reassociation-timeout 25 1
```

config wlan security ft

To configure 802.11r Fast Transition Roaming parameters, use the **config wlan security ft** command.

config wlan security ft {**enable** | **disable** | **reassociation-timeout** *timeout-in-seconds*} *wlan_id*

Syntax Description

enable	Enables 802.11r Fast Transition Roaming support.
disable	Disables 802.11r Fast Transition Roaming support.
reassociation-timeout	Configures reassociation deadline interval.
timeout-in-seconds	Reassociation timeout value, in seconds. The valid range is 1 to 100 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

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

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

The following example shows how to enable 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft enable 2
```

The following example shows how to set a reassociation timeout value of 20 seconds for 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft reassociation-timeout 20 2
```

save config

To save the controller configurations, use the **save config** command.

save config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to save the controller settings:

```
(Cisco Controller) > save config
Are you sure you want to save? (y/n) y
Configuration Saved!
```

Related Topics

show sysinfo, on page 458

Resetting the System Reboot Time

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

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, on page 344
reset system notify-time, on page 346

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.
no-swap	Boots from the active image.
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
7.6	This command was introduced in a release earlier than Release 7.6.

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, on page 344
reset system notify-time, on page 346

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

The following example shows how to cancel a scheduled reset:

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

Related Topics

reset system at, on page 344
reset system in, on page 344
reset system notify-time, on page 346

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

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

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

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

Related Topics

reset system at, on page 344
reset system in, on page 344

reset peer-system

To reset the peer controller, use the **reset peer-system** command.

reset peer-system

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to reset the peer controller:

```
> reset peer-system
```

show 802.11 cu-metrics

To display access point channel utilization metrics, use the **show 802.11 cu-metrics** command.

show 802.11 {**a** | **b**} **cu-metrics** *cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
cisco_ap	Access point name.

Command Default

None

Command History

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

The following is a sample output of the **show 802.11a cu-metrics** command:

```
(Cisco Controller) > show 802.11a cu-metrics AP1
AP Interface Mac:           30:37:a6:c8:8a:50
Measurement Duration:       90sec
 Timestamp               Thu Jan 27 09:08:48 2011
   Channel Utilization stats
   =================
     Picc (50th Percentile)..................... 0
     Pib (50th Percentile)...................... 76
     Picc (90th Percentile)..................... 0
     Pib (90th Percentile)...................... 77
 Timestamp               Thu Jan 27 09:34:34 2011
```

show advanced 802.11 l2roam

To display 802.11a or 802.11b/g Layer 2 client roaming information, use the **show advanced 802.11 l2roam** command.

show advanced 802.11 {**a** | **b**} **l2roam** {**rf-param** | **statistics**} *mac_address*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
rf-param	Specifies the Layer 2 frequency parameters.
statistics	Specifies the Layer 2 client roaming statistics.
mac_address	MAC address of the client.

Command Default

None

Command History

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

The following is a sample output of the **show advanced 802.11b l2roam rf-param** command:

```
(Cisco Controller) > show advanced 802.11b l2roam rf-param

L2Roam 802.11bg RF Parameters.....................
    Config Mode.................................. Default
    Minimum RSSI................................. -85
    Roam Hysteresis.............................. 2
    Scan Threshold............................... -72
    Transition time.............................. 5
```

show advanced send-disassoc-on-handoff

To display whether the WLAN controller disassociates clients after a handoff, use the **show advanced send-disassoc-on-handoff** command.

show advanced send-disassoc-on-handoff

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following is a sample output of the **show advanced send-disassoc-on-handoff** command:

```
(Cisco Controller) > show advanced send-disassoc-on-handoff
Send Disassociate on Handoff..................... Disabled
```

show advanced sip-preferred-call-no

To display the list of preferred call numbers, use the **show advanced sip-preferred-call-no** command.

show advanced sip-preferred-call-no

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following is a sample output of the **show advanced sip-preferred-call-no** command:

```
(Cisco Controller) > show advanced sip-preferred-call-no
Preferred Call Numbers List
Call Index            Preferred Call No
-----------           ------------------
1                      911
2                      100
3                      101
4                      102
5                      103
6                      104
```

show advanced sip-snooping-ports

To display the port range for call snooping, use the **show advanced sip-snooping-ports** command.

show advanced sip-snooping-ports

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following is a sample output of the **show advanced sip-snooping-ports** command:

```
(Cisco Controller) > show advanced sip-snooping-ports
 SIP Call Snoop Ports: 1000 - 2000
```

show arp kernel

To display the kernel Address Resolution Protocol (ARP) cache information, use the **show arp kernel** command.

show arp kernel

This command has no arguments or keywords.

Command Default

None

Command History

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

The following is a sample output of the **show arp kernel** command:

```
(Cisco Controller) > show arp kernel
IP address       HW type     Flags       HW address            Mask     Device
192.0.2.1        0x1         0x2         00:1A:6C:2A:09:C2     *        dtl0
192.0.2.8        0x1         0x6         00:1E:E5:E6:DB:56     *        dtl0
```

Related Topics

clear arp, on page 14
debug arp, on page 495
show route kernel, on page 449

show arp switch

To display the Cisco wireless LAN controller MAC addresses, IP addresses, and port types, use the **show arp switch** command.

show arp switch

Syntax Description

This command has no arguments or keywords.

Command History

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

The following is a sample output of the **show arp switch** command:

```
(Cisco Controller) > show arp switch
MAC Address          IP Address         Port      VLAN      Type
------------------- ---------------- ------------ ---- --------------------
xx:xx:xx:xx:xx:xx   xxx.xxx.xxx.xxx  service port    1
xx:xx:xx:xx:xx:xx   xxx.xxx.xxx.xxx  service port
xx:xx:xx:xx:xx:xx   xxx.xxx.xxx.xxx  service port
```

Related Topics

clear arp, on page 14
debug arp, on page 495
show arp kernel, on page 352

show avc applications

To display all the supported Application Visibility and Control (AVC) applications, use the **show avc applications** command.

show avc applications

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

AVC uses the Network-Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1500 Layer 4 to Layer 7 protocols.

The following is a sample output of the **show avc applications** command:

```
(Cisco Controller) > show avc applications

Application-Name            App-ID  Engine-ID  Selector-ID   Application-Group-Name
 ================            ======  =========  ===========   ======================
 3com-amp3                    538         3        629        other
 3com-tsmux                   977         3        106        obsolete
 3pc                          788         1         34        layer3-over-ip
 914c/g                      1109         3        211        net-admin
 9pfs                         479         3        564        net-admin
 acap                         582         3        674        net-admin
 acas                         939         3         62        other
 accessbuilder                662         3        888        other
 accessnetwork                607         3        699        other
 acp                          513         3        599        other
 acr-nema                     975         3        104        industrial-protocols
 active-directory            1194        13        473        other
 activesync                  1419        13        490        business-and-productivity-tools

 adobe-connect               1441        13        505        other
 aed-512                      963         3        149        obsolete
 afpovertcp                  1327         3        548        business-and-productivity-tools

 agentx                       609         3        705        net-admin
 alpes                        377         3        463        net-admin
 aminet                       558         3       2639        file-sharing
 an                           861         1        107        layer3-over-ip
----                          ----       ---      -----       -------------
```

show avc profile

To display Application Visibility and Control (AVC) profiles, use the **show avc profile** command.

show avc profile {**summary** | **detailed** *profile_name* }

Syntax Description

summary	Displays a summary of AVC profiles.
detailed	Displays the details of an AVC profile.
profile_name	Name of the AVC profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc profile summary** command.

```
(Cisco Controller) > show avc profile summary

 Profile-Name                    Number of Rules
  ============                    ==============
  profile 1                              3
  avc_profile2                           1
```

The following is a sample output of the **show avc profile detailed** command.

```
(Cisco Controller) > show avc profile detailed

  Application-Name          Application-Group-Name           Action  DSCP
  ================          ======================           ======  ====
  ftp                       file-sharing                      Drop      -
  flash-video               browsing                          Mark     10
  facebook                  browsing                          Mark     10

  Associated WLAN IDs       :
  Associated Remote LAN IDs :
  Associated Guest LAN IDs  :
```

show avc statistics application

To display the statistics of an application, use the **show avc statistics application** command.

show avc statistics application *application_name* **top-users** [**downstream wlan** | **upstream wlan** | **wlan**] [*wlan_id*] }

Syntax Description

application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-users	Displays AVC statistics for top application users.
downstream	(Optional) Displays statistics of top downstream applications.
wlan	(Optional) Displays AVC statistics of a WLAN.
wlan_id	WLAN identifier from 1 to 512.
upstream	(Optional) Displays statistics of top upstream applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics application** command:

```
(Cisco Controller) > show avc statistics application ftp top-users downstream wlan 1

  Client MAC            Client IP        WLAN ID  Packets   Bytes   Avg Pkt  Packets
Bytes       DSCP
  (Up/Down)                                       (n secs) (n secs)  Size    (Total)
(Total)   In  Out
  ===========           =========        ======   =======  =======  ======   =======
=======   === ===
  00:0a:ab:15:00:9c(U) 172.16.31.156        1         16        91     5         43
  338     0   0
                  (D) 172.16.31.156        1         22      5911   268         48
 6409     0   0
  00:0a:ab:15:00:5a(U) 172.16.31.90         1          7        39     5         13
   84     0   0
                  (D) 172.16.31.90         1         12      5723   476         18
 5869     0   0
  00:0a:ab:15:00:60(U) 172.16.31.96         1         19       117     6         75
 8666     0   0
                  (D) 172.16.31.96         1         19      4433   233         83
 9595     0   0
  00:0a:ab:15:00:a4(U) 172.16.31.164        1         18       139     7         21
  161     0   0
                  (D) 172.16.31.164        1         23      4409   191         24
 4439     0   0
  00:0a:ab:15:00:48(U) 172.16.31.72         1         21      2738   130         21
 2738     0   0
                  (D) 172.16.31.72         1         22      4367   198         22
```

```
4367     0   0
 00:0a:ab:15:00:87(U) 172.16.31.135        1          11         47      4          49
 301      0   0
                  (D) 172.16.31.135        1          12       4208    350          48
7755     0   0
 00:0a:ab:15:00:92(U) 172.16.31.146        1          10         73      7          11
  84      0   0
                  (D) 172.16.31.146        1           9       4168    463          11
4201     0   0
 00:0a:ab:15:00:31(U) 172.16.31.49         1          11         95      8          34
 250      0   0
                  (D) 172.16.31.49         1          18       3201    177          43
3755     0   0
 00:0a:ab:15:00:46(U) 172.16.31.70         1           7         47      6          20
 175      0   0
                  (D) 172.16.31.70         1          10       3162    316          23
3448     0   0
 00:0a:ab:15:00:b3(U) 172.16.31.179        1          10         85      8          34
 241      0   0
```

show avc statistics client

To display the client Application Visibility and Control (AVC) statistics, use the **show avc statistics client** command.

show avc statistics client *client_MAC* {**application** *application_name* | **top-apps** [**upstream** | **downstream**]}

Syntax Description

client_MAC	MAC address of the client.
application	Displays AVC statistics for an application.
application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-apps	Displays AVC statistics for top applications.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics client** command:

```
(Cisco Controller) > show avc statistics client 00:0a:ab:15:00:01 application http

 Description                   Upstream      Downstream
  ===========                   ========      ==========
  Number of Packtes(n secs)         5059            6369
  Number of Bytes(n secs)         170144         8655115
  Average Packet size(n secs)         33            1358
  Total Number of Packtes         131878          150169
  Total Number of Bytes          6054464       205239972
  DSCP Incoming packet                16               0
  DSCP Outgoing Packet                16               0
```

The following is a sample output of the **show avc statistics client** command.

```
(Cisco Controller) > show avc statistics client 00:0a:ab:15:00:01 top-apps

  Application-Name           Packets   Bytes    Avg Pkt  Packets    Bytes    DSCP DSCP
      (Up/Down)              (n secs)  (n secs)  Size    (Total)   (Total)    In   Out
  ================           =======   ======   ======   =======   ======    ====  ====
  http                  (U)     6035   637728    105       6035     637728    16    16
                        (D)     5420  7218796   1331       5420    7218796     0     0
  ggp                   (U)     1331  1362944   1024       1331    1362944     0     0
                        (D)        0        0      0          0          0     0     0
  smp                   (U)     1046  1071104   1024       1046    1071104     0     0
                        (D)        0        0      0          0          0     0     0
  vrrp                  (U)      205   209920   1024        205     209920     0     0
```

	(D)	0	0	0	0	0	0	0
bittorrent	(U)	117	1604	13	117	1604	0	0
	(D)	121	70469	582	121	70469	0	0
icmp	(U)	0	0	0	0	0	0	0
	(D)	72	40032	556	72	40032	48	48
edonkey	(U)	112	4620	41	112	4620	0	0
	(D)	105	33076	315	105	33076	0	0
dns	(U)	10	380	38	10	380	0	0
	(D)	7	1743	249	7	1743	0	0
realmedia	(U)	2	158	79	2	158	24	24
	(D)	2	65	32	2	65	0	0

show avc statistics guest-lan

To display the Application Visibility and Control (AVC) statistics of a guest LAN, use the **show avc statistics guest-lan** command.

show avc statistics guest-lan *guest-lan_id* {**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}

Syntax Description

guest-lan_id	Guest LAN identifier from 1 to 5.
application	Displays AVC statistics for an application.
application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-app-groups	Displays AVC statistics for top application groups.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.
top-apps	Displays AVC statistics for top applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics** command.

```
(Cisco Controller) > show avc statistics guest-lan 1

 Application-Name             Packets   Bytes   Avg Pkt  Packets      Bytes
   (Up/Down)                  (n secs) (n secs)  Size    (Total)      (Total)
 ================             =======  ======    ======   ======      =======
 unclassified            (U)  191464    208627     1    92208613  11138796586
                         (D)  63427  53440610   842    16295621   9657054635
 ftp                     (U)    805     72880    90      172939     11206202
                         (D)    911     58143    63      190900     17418653
 http                    (U)  264904  12508288    47    27493945   2837672192
                         (D)  319894  436915253  1365    29850934  36817587924
 gre                     (U)      0         0     0    10158872  10402684928
                         (D)      0         0     0           0           0
 icmp                    (U)      1        40    40         323        98476
                         (D)   7262   4034576   555     2888266   1605133372
 ipinip                  (U)  62565  64066560  1024    11992305  12280120320
                         (D)      0         0     0           0           0
 imap                    (U)   1430     16798    11      305161      3795766
                         (D)   1555    576371   370      332290    125799465
 irc                     (U)      9        74     8        1736         9133
                         (D)     11       371    33        1972       173381
 nntp                    (U)     22       158     7        1705         9612
                         (D)     22       372    16        2047       214391
```

show avc statistics remote-lan

To display the Application Visibility and Control (AVC) statistics of a remote LAN, use the **show avc statistics remote-lan** command.

show avc statistics remote-lan *remote-lan_id* { **application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**] }

Syntax Description

remote-lan_id	Remote LAN identifier from 1 to 512.
application	Displays AVC statistics for an application.
application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-app-groups	Displays AVC statistics for top application groups.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.
top-apps	Displays AVC statistics for top applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics remote-lan** command.

```
(Cisco Controller) > show avc statistics remote-lan 1

 Application-Name             Packets   Bytes   Avg Pkt  Packets      Bytes
   (Up/Down)                  (n secs) (n secs)  Size    (Total)      (Total)
 ================             =======  ======    ======   ======      =======
 unclassified            (U)  191464    208627     1    92208613  11138796586
                         (D)  63427  53440610   842    16295621   9657054635
 ftp                     (U)    805     72880    90      172939     11206202
                         (D)    911     58143    63      190900     17418653
 http                    (U)  264904  12508288    47    27493945   2837672192
                         (D)  319894  436915253  1365    29850934  36817587924
 gre                     (U)      0         0     0    10158872  10402684928
                         (D)      0         0     0           0           0
 icmp                    (U)      1        40    40         323        98476
                         (D)   7262   4034576   555     2888266   1605133372
 ipinip                  (U)  62565  64066560  1024    11992305  12280120320
                         (D)      0         0     0           0           0
 imap                    (U)   1430     16798    11      305161      3795766
                         (D)   1555    576371   370      332290    125799465
 irc                     (U)      9        74     8        1736         9133
                         (D)     11       371    33        1972       173381
 nntp                    (U)     22       158     7        1705         9612
                         (D)     22       372    16        2047       214391
```

show avc statistics top-apps

To display the Application Visibility and Control (AVC) statistics for the most used applications, use the **show avc statistics top-apps** command.

show avc statistics top-apps [**upstream** | **downstream**]

Syntax Description

upstream	(Optional) Displays statistics of the most used upstream applications.
downstream	(Optional) Displays statistics of the most used downstream applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics top-apps** command:

```
(Cisco Controller) > show avc statistics top-apps

Application-Name             Packets     Bytes   Avg Pkt     Packets         Bytes
   (Up/Down)                 (n secs)   (n secs)  Size       (Total)        (Total)
================             =======    =======  =======     =======        ========
http                   (U)    204570   10610912     51      28272539      2882294016
                       (D)    240936  327624221   1359      30750570     38026889010
realmedia              (U)       908      62154     68        400698        26470359
                       (D)    166694  220522943   1322      35802836     47131836785
mpls-in-ip             (U)     77448   79306752   1024      10292787     10539813888
                       (D)         0          0      0             0              0
fire                   (U)     70890   72591360   1024      10242484     10488303616
                       (D)         0          0      0             0              0
pipe                   (U)     68296   69935104   1024      10224255     10469637120
                       (D)         0          0      0             0              0
gre                    (U)     60982   62445568   1024      10340221     10588386304
                       (D)         0          0      0             0              0
crudp                  (U)     26430   27064320   1024      10109812     10352447488
                       (D)         0          0      0             0              0
rtp                    (U)         0          0      0             0              0
                       (D)      7482    9936096   1328       2603923      3458009744
icmp                   (U)         0          0      0           323           98476
                       (D)     10155    5640504    555       2924693      1625363564
```

Related Commands

config avc profile delete

config avc profile create

config avc profile rule

config wlan avc

show avc profile

show avc applications

show avc statistics client

show avc statistics wlan

show avc statistics applications

show avc statistics guest-lan

show avc statistics remote-lan

debug avc error

debug avc events

show avc statistics wlan

To display the Application Visibility and Control (AVC) statistics of a WLAN, use the **show avc statistics wlan** command.

show avc statistics wlan *wlan_id* {**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}

Syntax Description

wlan_id	WLAN identifier from 1 to 512.
application	Displays AVC statistics for an application.
application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-app-groups	Displays AVC statistics for top application groups.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.
top-apps	Displays AVC statistics for top applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics** command.

```
(Cisco Controller) >show avc statistics wlan 1

 Application-Name            Packets   Bytes   Avg Pkt  Packets      Bytes
   (Up/Down)                 (n secs) (n secs)  Size    (Total)      (Total)
 ================            =======  ======    ======   ======      =======
 unclassified           (U)  191464    208627     1    92208613  11138796586
                        (D)  63427  53440610   842    16295621   9657054635
 ftp                    (U)    805     72880    90      172939     11206202
                        (D)    911     58143    63      190900     17418653
 http                   (U)  264904  12508288    47    27493945   2837672192
                        (D)  319894  436915253  1365    29850934  36817587924
 gre                    (U)      0         0     0    10158872  10402684928
                        (D)      0         0     0           0           0
 icmp                   (U)      1        40    40         323        98476
                        (D)   7262   4034576   555     2888266   1605133372
 ipinip                 (U)  62565  64066560  1024    11992305  12280120320
                        (D)      0         0     0           0           0
 imap                   (U)   1430     16798    11      305161      3795766
                        (D)   1555    576371   370      332290    125799465
 irc                    (U)      9        74     8        1736         9133
                        (D)     11       371    33        1972       173381
 nntp                   (U)     22       158     7        1705         9612
                        (D)     22       372    16        2047       214391
```

The following is a sample output of the **show avc statistics wlan** command.

```
(Cisco Controller) >show avc statistics wlan 1 application ftp

 Description                    Upstream    Downstream
  ===========                    ========    ==========
  Number of Packtes(n secs)             0             0
  Number of Bytes(n secs)               0             0
  Average Packet size(n secs)           0             0
  Total Number of Packtes           32459         64888
  Total Number of Bytes               274      94673983
```

Related Topics

config wlan avc

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

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 band-select

To display band selection information, use the **show band-select** command.

show band-select

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following is a sample output of the **show band-select** command:

```
(Cisco Controller) > show band-select
Band Select Probe Response..................... per WLAN enabling
   Cycle Count..................................... 3 cycles
   Cycle Threshold................................. 200 milliseconds
   Age Out Suppression............................. 20 seconds
   Age Out Dual Band............................... 60 seconds
   Client RSSI..................................... -80 dBm
```

Related Commands

config band-select

config wlan band-select

show buffers

To display buffer information of the controller, use the **show buffers** command.

show buffers

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following is a sample output of the **show buffers** command:

```
(Cisco Controller) > show buffers
Pool[00]: 16 byte chunks
    chunks in pool:    50000
    chunks in use:     9196
    bytes in use:      147136
    bytes requested:   73218 (73918 overhead bytes)
Pool[01]: 64 byte chunks
    chunks in pool:    50100
    chunks in use:     19222
    bytes in use:      1230208
    bytes requested:   729199 (501009 overhead bytes)
Pool[02]: 128 byte chunks
    chunks in pool:    26200
    chunks in use:     9861
    bytes in use:      1262208
    bytes requested:   848732 (413476 overhead bytes)
Pool[03]: 256 byte chunks
    chunks in pool:    3000
    chunks in use:     596
    bytes in use:      152576
    bytes requested:   93145 (59431 overhead bytes)
Pool[04]: 384 byte chunks
    chunks in pool:    6000
    chunks in use:     258
    bytes in use:      99072
    bytes requested:   68235 (30837 overhead bytes)
Pool[05]: 512 byte chunks
    chunks in pool:    18700
    chunks in use:     18667
    bytes in use:      9557504
    bytes requested:   7933814 (1623690 overhead bytes)
Pool[06]: 1024 byte chunks
    chunks in pool:    3500
    chunks in use:     94
    bytes in use:      96256
    bytes requested:   75598 (20658 overhead bytes)
Pool[07]: 2048 byte chunks
    chunks in pool:    1000
    chunks in use:     54
    bytes in use:      110592
    bytes requested:   76153 (34439 overhead bytes)
Pool[08]: 4096 byte chunks
    chunks in pool:    1000
```

```
    chunks in use:     47
    bytes in use:      192512
    bytes requested:   128258 (64254 overhead bytes)
Raw Pool:
    chunks in use:     256
    bytes requested:   289575125
```

show cac voice stats

To view the detailed voice CAC statistics of the 802.11a or 802.11b radio, use the **show cac voice stats** command.

show cac voice stats {**802.11a** | **802.11b**}

Syntax Description

802.11a	Displays detailed voice CAC statistics for 802.11a.
802.11b	Displays detailed voice CAC statistics for 802.11b/g.

Command History

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

The following is a sample output of the **show cac voice stats 802.11b** command:

```
(Cisco Controller) > show cac voice stats 802.11b

WLC Voice Call Statistics for 802.11b Radio

WMM TSPEC CAC Call Stats
  Total num of Calls in progress.................. 0
  Num of Roam Calls in progress.................. 0
  Total Num of Calls Admitted..................... 0
  Total Num of Roam Calls Admitted................ 0
  Total Num of exp bw requests received.......... 0
  Total Num of exp bw requests Admitted.......... 0
  Total Num of Calls Rejected..................... 0
  Total Num of Roam Calls Rejected................ 0
  Num of Calls Rejected due to insufficent 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 Roam Calls in progress.................. 0
  Total Num of Calls Admitted..................... 0
  Total Num of Roam Calls Admitted................ 0
  Total Num of Preferred Calls Received.......... 0
  Total Num of Preferred Calls Admitted.......... 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
KTS based CAC Call Stats
  Total Num of Calls in progress.................. 0
  Num of Roam Calls in progress.................. 0
  Total Num of Calls Admitted..................... 0
  Total Num of Roam Calls Admitted................ 0
  Total Num of Calls Rejected(Insuff BW)......... 0
  Total Num of Roam Calls Rejected(Insuff BW).... 0
```

Related Topics

config 802.11 cac defaults, on page 56
config 802.11 cac multimedia, on page 68

show cac voice summary

To view the list of all APs with brief voice statistics (includes bandwidth used, maximum bandwidth available, and the number of calls information), use the **show cac voice summary** command.

show cac voice summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following is a sample output of the **show cac voice summary** command:

```
(Cisco Controller) > show cac voice summary
    AP Name          Slot#   Radio  BW Used/Max  Calls
-----------------  -------  -----  -----------  -----
APc47d.4f3a.3547     0      11b/g     0/23437    0
      1      11a    1072/23437    1
```

Related Topics

show mesh cac, on page 425

show cac video stats

To view the detailed video CAC statistics of the 802.11a or 802.11b radio, use the **show cac video stats** command.

show cac video stats {**802.11a** | **802.11b**}

Syntax Description

802.11a	Displays detailed video CAC statistics for 802.11a.
802.11b	Displays detailed video CAC statistics for 802.11b/g.

Command History

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

The following is a sample output of the **show cac video stats 802.11b** command:

```
(Cisco Controller) > show cac video stats 802.11b

WLC Video Call Statistics for 802.11b Radio

WMM TSPEC CAC Call Stats
  Total num of Calls in progress.............. 0
  Num of Roam Calls in progress............... 0
  Total Num of Calls Admitted................. 0
  Total Num of Roam Calls Admitted............ 0
  Total Num of Calls Rejected................. 0
  Total Num of Roam Calls Rejected............ 0
  Num of Calls Rejected due to insufficent 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 Roam Calls in progress............... 0
  Total Num of Calls Admitted................. 0
  Total Num of Roam Calls Admitted............ 0
  Total Num of Calls Rejected(Insuff BW)......... 0
  Total Num of Roam Calls Rejected(Insuff BW).... 0
```

Related Commands

config 802.11 cac voice

config 802.11 cac defaults

config 802.11 cac video

config 802.11 cac multimedia

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video load-based

config 802.11 cac video cac-method

config 802.11 cac video sip

show cac video summary

To view the list of all access points with brief video statistics (includes bandwidth used, maximum bandwidth available, and the number of calls information), use the **show cac video summary** command.

show cac video summary

Syntax Description

This command has no arguments or keywords.

Command History

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

The following is a sample output of the **show cac video summary** command:

```
(Cisco Controller) > show cac video summary

    AP Name          Slot#   Radio  BW Used/Max  Calls
-----------------  -------  -----  -----------  -----
AP001b.d571.88e0     0      11b/g     0/10937    0
                     1      11a       0/18750    0
AP5_1250             0      11b/g     0/10937    0
                     1      11a       0/18750    0
```

Related Commands

config 802.11 cac voice

config 802.11 cac defaults

config 802.11 cac video

config 802.11 cac multimedia

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video load-based

config 802.11 cac video cac-method

config 802.11 cac video sip

show cdp

To display the status and details of the Cisco Discovery Protocol (CDP), use the **show cdp** command.

show cdp {**neighbors** [**detail**] | **entry all** | **traffic**}

Syntax Description

neighbors	Displays a list of all CDP neighbors on all interfaces.
detail	(Optional) Displays detailed information of the controller's CDP neighbors. This command shows only the CDP neighbors of the controller; it does not show the CDP neighbors of the controller's associated access points.
entry all	Displays all CDP entries in the database.
traffic	Displays CDP traffic information.

Command Default

None

Command History

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

The following is a sample output of the **show cdp** command:

```
(Cisco Controller) > show cdp
CDP counters :
Total packets output: 0, Input: 0
Chksum error: 0
No memory: 0, Invalid packet: 0,
```

Related Commands

config cdp

config ap cdp

show ap cdp

show certificate compatibility

To display whether or not certificates are verified as compatible in the Cisco wireless LAN controller, use the **show certificate compatibility** command.

show certificate compatibility

Syntax Description

This command has no arguments or keywords.

Command History

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

The following is a sample output of the **show certificate compatibility** command:

```
(Cisco Controller) > show certificate compatibility
Certificate compatibility mode:.............. off
```

Related Topics

config certificate lsc, on page 122
show certificate lsc, on page 378
show certificate summary, on page 381
show local-auth certificates, on page 420
config certificate, on page 121

show certificate lsc

To verify that the controller has generated a Locally Significant Certificate (LSC), use the **show certificate lsc summary** command.

show certificate lsc {**summary** | **ap-provision**}

Syntax Description

summary	Displays a summary of LSC certificate settings and certificates.
ap-provision	Displays details about the access points that are provisioned using the LSC.

Command Default

None

Command History

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

The following is a sample output of the **show certificate lsc summary** command:

```
(Cisco Controller) > show certificate lsc summary
LSC Enabled..................................... Yes
LSC CA-Server................................... http://10.0.0.1:8080/caserver
LSC AP-Provisioning............................. Yes
Provision-List.............................. Not Configured
LSC Revert Count in AP reboots.............. 3
LSC Params:
Country..................................... 4
State....................................... ca
City........................................ ss
Orgn........................................ org
Dept........................................ dep
Email....................................... dep@co.com
KeySize..................................... 390
LSC Certs:
CA Cert..................................... Not Configured
RA Cert..................................... Not Configured
```

This example shows how to display the details about the access points that are provisioned using the LSC:

```
(Cisco Controller) > show certificate lsc ap-provision
LSC AP-Provisioning............................. Yes
Provision-List.............................. Present
Idx Mac Address
--- -------------
1 00:18:74:c7:c0:90
```

Related Topics

config certificate lsc, on page 122
show certificate compatibility, on page 377

show local-auth certificates, on page 420
show certificate summary, on page 381
config certificate, on page 121

show certificate ssc

To view the Self Signed Device Certificate (SSC) and hash key of the virtual controller, use the **show certificate ssc** command.

show certificate ssc

Syntax Description

This command has no arguments or keywords.

Command History

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

The following is a sample output of the **show certificate ssc** command :

```
(Cisco Controller) > show certificate ssc
 SSC Hash validation.............................. Enabled.

 SSC Device Certificate details:

         Subject Name :
                 C=US, ST=California, L=San Jose, O=Cisco Virtual Wireless LAN Controller,
                 CN=DEVICE-vWLC-AIR-CTVM-K9-000C297F2CF7, MAILTO=support@vwlc.com

         Validity :
                 Start : 2012 Jul 23rd, 15:47:53 GMT
                 End   : 2022 Jun  1st, 15:47:53 GMT

         Hash key : 5870ffabb15de2a617132bafcd73
```

Related Topics

config certificate ssc, on page 124
show mobility group member, on page 432
config mobility group member, on page 196

show certificate summary

To verify that the controller has generated a certificate, use the **show certificate summary** command.

show certificate summary

Syntax Description

This command has no arguments or keywords.

Command History

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

The following is a sample output of the **show certificate summary** command:

```
(Cisco Controller) > show certificate summary
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:.................... off
```

Related Topics

config certificate lsc, on page 122
show certificate compatibility, on page 377
show local-auth certificates, on page 420
config certificate, on page 121

show client calls

To display the total number of active or rejected calls on the controller, use the **show client calls** command.

show client calls {**active** | **rejected**} {**802.11a** | **802.11bg** | **all**}

Syntax Description

active	Specifies active calls.
rejected	Specifies rejected calls.
802.11a	Specifies the 802.11a network.
802.11bg	Specifies the 802.11b/g network.
all	Specifies both the 802.11a and 802.11b/g network.

Command Default

None

Command History

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

The following is a sample output of the **show client calls active 802.11a** command :

```
(Cisco Controller) > show client calls active 802.11a
Client MAC               Username         Total Call            AP Name         Radio Type
                                          Duration (sec)
--------------------    ---------         ----------       ---------------      ----------
00:09: ef: 02:65:70        abc               45            VJ-1240C-ed45cc        802.11a
00:13: ce: cc: 51:39       xyz               45                AP1130-a416        802.11a
00:40:96: af: 15:15        def               45                AP1130-a416        802.11a
00:40:96:b2:69: df         def               45                AP1130-a416        802.11a
Number of Active Calls ----------------------------------- 4
```

Related Topics

debug voice-diag, on page 516

show client roam-history

To display the roaming history of a specified client, use the **show client roam-history** command.

show client roam-history *mac_address*

Syntax Description

mac_address	Client MAC address.

Command Default

None

Command History

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

The following is a sample output of the **show client roam-history** command:

```
(Cisco Controller) > show client roam-history 00:14:6c:0a:57:77
```

show client summary

To display a summary of clients associated with a Cisco lightweight access point, use the **show client summary** command.

show client summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

Usage Guidelines

Use **show client ap** command to list the status of automatically disabled clients. Use the **show exclusionlist** command to display clients on the exclusion list.

The following example shows how to display a summary of the active clients:

```
(Cisco Controller) > show client summary
Number of Clients.............................. 24
Number of PMIPV6 Clients....................... 200
MAC Address       AP Name           Status        WLAN/GLAN/RLAN Auth Protocol         Port
 Wired  PMIPV6
----------------- ----------------- ------------- -------------- ---- ---------------- ----
 -----  ------

00:00:15:01:00:01 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a          13
  No      Yes
00:00:15:01:00:02 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a          13
  No      No
00:00:15:01:00:03 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a          13
  No      Yes
00:00:15:01:00:04 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a          13
  No      No
```

show client summary guest-lan

To display the active wired guest LAN clients, use the **show client summary guest-lan** command.

show client summary guest-lan

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following is a sample output of the **show client summary guest-lan** command:

```
(Cisco Controller) > show client summary guest-lan
Number of Clients................................ 1
MAC Address       AP Name      Status         WLAN  Auth   Protocol  Port Wired
-----------       ---------    ----------     ----  ----   --------  ---- -----
00:16:36:40:ac:58  N/A         Associated        1    No      802.3     1   Yes
```

Related Commands

show client summary

show client tsm

To display the client traffic stream metrics (TSM) statistics, use the **show client tsm** command.

show client tsm 802.11{**a** | **b**} *client_mac* {*ap_mac* | **all**}

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11 b/g network.
client_mac	MAC address of the client.
ap_mac	MAC address of the tsm access point.
all	Specifies the list of all access points to which the client has associations.

Command Default

None

Command History

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

The following is a sample output of the **show client tsm 802.11a** command:

```
(Cisco Controller) > show client tsm 802.11a xx:xx:xx:xx:xx:xx all
AP Interface MAC: 00:0b:85:01:02:03
Client Interface Mac:               00:01:02:03:04:05
Measurement Duration:               90 seconds
  Timestamp                           1st Jan 2006, 06:35:80
    UpLink Stats
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec).............................10
      Maximum Lost Packet count(5sec)............................5
      Average Lost Packet count(5secs)...........................2
    DownLink Stats
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec).............................10
      Maximum Lost Packet count(5sec)............................5
      Average Lost Packet count(5secs)...........................2
```

Related Commands

show client ap

show client detail

show client summary

show client username

To display the client data by the username, use the **show client username** command.

show client username *username*

Syntax Description

username	Client's username. You can view a list of the first eight clients that are in RUN state associated to controller's access points.

Command Default

None

Command History

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

The following is a sample output of the **show client username** command:

```
(Cisco Controller) > show client username local

MAC Address        AP Name            Status         WLAN  Auth  Protocol          Port
Device Type
-----------------  -----------------  -------------  ----  ----  ----------------  ----
-----------

12:22:64:64:00:01  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
Unknown
12:22:64:64:00:02  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
Unknown
12:22:64:64:00:03  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
Unknown
12:22:64:64:00:04  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
Unknown
12:22:64:64:00:05  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
Unknown
12:22:64:64:00:06  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
Unknown
12:22:64:64:00:07  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
Unknown
12:22:64:64:00:08  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
Unknown
```

show client voice-diag

To display voice diagnostics statistics, use the **show client voice-diag** command.

show client voice-diag {**quos-map** | **roam-history** | **rssi** | **status** | **tspec**}

Syntax Description

quos-map	Displays information about the QoS/DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.
roam-history	Displays information about history of the last three roamings. The output contains the timestamp, access point associated with the roaming, the roaming reason, and if there is a roaming failure, the reason for the roaming failure.
rssi	Displays the client's RSSI values in the last 5 seconds when voice diagnostics are enabled.
status	Displays the status of voice diagnostics for clients.
tspec	Displays TSPEC for the voice diagnostic for clients.

Command Default

None

Command History

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

The following is a sample output of the **show client voice-diag status** command:

```
(Cisco Controller) > show client voice-diag status
Voice Diagnostics Status: FALSE
```

Related Commands

show client ap

show client detail

show client summary

debug voice-diag

show coredump summary

To display a summary of the controller's core dump file, use the **show coredump summary** command.

show coredump summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following is a sample output of the **show coredump summary** command:

```
(Cisco Controller) > show coredump summary
Core Dump is enabled
FTP Server IP..................................... 10.10.10.17
FTP Filename...................................... file1
FTP Username...................................... ftpuser
FTP Password...................................... *********
```

Related Commands

config coredump

config coredump ftp

config coredump username

show cpu

To display current WLAN controller CPU usage information, use the **show cpu** command.

show cpu

Syntax Description

This command has no arguments or keywords.

Command History

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

The following is a sample output of the **show cpu** command:

```
(Cisco Controller) > show cpu
Current CPU load: 2.50%
```

show custom-web

To display all the web authentication customization information, use the command.

Syntax Description

all	Display all Web-Auth customization information.
remote-lan	Display per WLAN Web-Auth customization information.
guest-lan	Display per Guest LAN Web-Auth customization information.
sleep-client	Display all Web-Auth Sleeping Client entries summary.
webauth-bundle	Display the content of Web-Auth Bundle.
wlan	Display per WLAN Web-Auth customization information.

Command History

Release	Modification
7.6	This command was introduced in the release earlier than 7.6.
8.2	This command was modified and the all, remote-lan, guest-lan, sleep-client, webauth-bundle, and wlan keywords are added.

The following is a sample output of the command:

```
(Cisco Controller) > show custom-web all
Radius Authentication Method..................... PAP
Cisco Logo....................................... Enabled
CustomLogo....................................... None
Custom Title..................................... None
Custom Message................................... None
Custom Redirect URL.............................. None
Web Authentication Type.......................... Internal Default
Logout-popup..................................... Enabled
External Web Authentication URL.................. None
```

show database summary

To display the maximum number of entries in the database, use the **show database summary** command.

show database summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

The following is a sample output of the **show database summary** command:

```
(Cisco Controller) > show database summary
Maximum Database Entries..................... 2048
Maximum Database Entries On Next Reboot...... 2048
Database Contents
    MAC Filter Entries..................... 2
    Exclusion List Entries................. 0
    AP Authorization List Entries.......... 1
    Management Users....................... 1
    Local Network Users.................... 1
        Local Users........................ 1
        Guest Users........................ 0
    Total.................................. 5
```

Related Commands

config database size

show dhcp

To display the internal Dynamic Host Configuration Protocol (DHCP) server configuration, use the **show dhcp** command.

show dhcp {**leases** | **summary** | *scope*}

Syntax Description

leases	Displays allocated DHCP leases.
summary	Displays DHCP summary information.
scope	Name of a scope to display the DHCP information for that scope.

Command Default

None

Command History

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

The following example shows how to display the allocated DHCP leases:

```
(Cisco Controller) >show dhcp leases
No leases allocated.
```

The following example shows how to display the DHCP summary information:

```
(Cisco Controller) >show dhcp summary
Scope Name           Enabled          Address Range
003                    No           0.0.0.0 -> 0.0.0.0
```

The following example shows how to display the DHCP information for the scope 003:

```
(Cisco Controller) >show dhcp 003
Enabled..................................... No
Lease Time.................................. 0
Pool Start.................................. 0.0.0.0
Pool End.................................... 0.0.0.0
Network..................................... 0.0.0.0
Netmask..................................... 0.0.0.0
Default Routers............................. 0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain..................................
DNS......................................... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers........................ 0.0.0.0 0.0.0.0 0.0.0.0
```

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

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 dhcp proxy

To display the status of DHCP proxy handling, use the **show dhcp proxy** command.

show dhcp proxy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to display the status of DHCP proxy information:

```
(Cisco Controller) >show dhcp proxy

DHCP Proxy Behavior: enabled
```

show dhcp timeout

To display the DHCP timeout value, use the **show dhcp timeout** command.

show dhcp timeout

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to display the DHCP timeout value:

```
(Cisco Controller) >show dhcp timeout

DHCP Timeout (seconds)..... 10
```

show flow exporter

To display the details or the statistics of the flow exporter, use the **show flow exporter** command.

show flow exporter {**summary** | **statistics**}

Syntax Description

summary	Displays a summary of the flow exporter.
statistics	Displays the statistics of flow exporters such as the number of records sent, or the time when the last record was sent.

Command Default

None

Command History

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

The following is a sample output of the **show flow exporter summary** command:

```
(Cisco Controller) > show flow exporter summary
 Exporter-Name            Exporter-IP     Port
  =============            ===========     =====
  expo1                    9.9.120.115       800
```

show flow monitor summary

To display the details of the NetFlow monitor, use the **show flow monitor summary** command.

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

Usage Guidelines

Netflow record monitoring and export are used for integration with an NMS or any Netflow analysis tool.

The following is a sample output of the **show flow monitor summary**:

```
(Cisco Controller) > show flow monitor summary
Monitor-Name             Exporter-Name            Exporter-IP      Port  Record Name
============             =============            ===========      ====  ===========
 mon1                     expo1                   9.9.120.115     800
ipv4_client_app_flow_record
```

show guest-lan

To display the configuration of a specific wired guest LAN, use the **show guest-lan** command.

show guest-lan *guest_lan_id*

Syntax Description

guest_lan_id	ID of the selected wired guest LAN.

Command Default

None

Command History

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

Usage Guidelines

To display all wired guest LANs configured on the controller, use the **show guest-lan summary** command.

The following is a sample output of the **show guest-lan** *guest_lan_id* command:

```
(Cisco Controller) >show guest-lan 2
Guest LAN Identifier..................... 1
Profile Name............................. guestlan
Network Name (SSID)...................... guestlan
Status................................... Enabled
AAA Policy Override...................... Disabled
Number of Active Clients................. 1
Exclusionlist Timeout.................... 60 seconds
Session Timeout.......................... Infinity
Interface................................ wired
Ingress Interface........................ wired-guest
WLAN ACL................................. unconfigured
DHCP Server.............................. 10.20.236.90
DHCP Address Assignment Required......... Disabled
Quality of Service....................... Silver (best effort)
Security
 Web Based Authentication................ Enabled
 ACL..................................... Unconfigured
 Web-Passthrough......................... Disabled
 Conditional Web Redirect................ Disabled
 Auto Anchor............................. Disabled
Mobility Anchor List
GLAN ID IP Address Status
```

show invalid-config

To see any ignored commands or invalid configuration values in an edited configuration file, use the **show invalid-config** command.

show invalid-config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

Usage Guidelines

You can enter this command only before the **clear config** or **save config** command.

The following is a sample output of the **show invalid-config** command:

```
(Cisco Controller) > show invalid-config
config wlan peer-blocking drop 3
config wlan dhcp_server 3 192.168.0.44 required
```

show inventory

To display a physical inventory of the Cisco wireless LAN controller, use the **show inventory** command.

show inventory

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

Usage Guidelines

Some wireless LAN controllers may have no crypto accelerator (VPN termination module) or power supplies listed because they have no provisions for VPN termination modules or power supplies.

The following is a sample output of the **show inventory** command:

```
(Cisco Controller) > show inventory
Burned-in MAC Address.......................... 50:3D:E5:1A:31:A0
Power Supply 1................................. Present, OK
Power Supply 2................................. Absent
Maximum number of APs supported................ 500
NAME: "Chassis"    , DESCR: "Cisco 5500 Series Wireless LAN Controller"
PID: AIR-CT5508-K9,  VID: V01,  SN: XXXXXXXXXXX
```

show license agent

To display the license agent counter and session information on the Cisco 5500 Series Controller, use the **show license agent** command.

show license agent {**counters** | **sessions**}

Syntax Description

counters	Displays license agent counter information.
sessions	Displays session information.

Command Default

None

Command History

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

The following is a sample output of the **show license agent counters** command:

```
(Cisco Controller) > show license agent counters
License Agent Counters
Request Messages Received:0: Messages with Errors:0
Request Operations Received:0: Operations with Errors:0
Notification Messages Sent:0: Transmission Errors:0: Soap Errors:0
```

The following is a sample output of the **show license agent sessions** command:

```
(Cisco Controller) > show license agent sessions
License Agent Sessions: 0 open, maximum is 9
```

Related Commands

config license agent

clear license agent

show license all

show license detail

show license feature

show license image-level

show license summary

show license all

To display information for all licenses on the Cisco WLCs, use the **show license all** command.

show license all

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display all the licenses:

```
> show license all
License Store: Primary License Storage
StoreIndex:  0  Feature: wplus-ap-count   Version: 1.0
        License Type: Permanent
        License State: Inactive
        License Count: 12/0/0
        License Priority: Medium
StoreIndex:  1  Feature: base   Version: 1.0
        License Type: Permanent
        License State: Active, Not in Use
        License Count: Non-Counted
        License Priority: Medium
StoreIndex:  2  Feature: wplus   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
License Store: Evaluation License Storage
StoreIndex:  0  Feature: wplus   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  6 weeks  6 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  1  Feature: wplus-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  2 weeks  3 days
            Expiry date: Thu Jun 25 18:09:43 2009
        License Count: 250/250/0
        License Priority: High
StoreIndex:  2  Feature: base   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  4 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  3  Feature: base-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  3 days
        License Count: 250/0/0
        License Priority: Low
```

show license capacity

To display the maximum number of access points allowed for this license on the Cisco 5500 Series Controller, the number of access points currently joined to the controller, and the number of access points that can still join the controller, use the **show license capacity** command.

show license capacity

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the license capacity:

```
> show license capacity
Licensed Feature    Max Count         Current Count     Remaining Count
------------------------------------------------------------------------
AP Count            250               47                203
```

Related Commands

license install

show license all

show license detail

show license feature

show license image-level

show license summary

license modify priority

show license evaluation

show license detail

To display details of a specific license on the Cisco 5500 Series Controller, use the **show license detail** command.

show license detail *license-name*

Syntax Description

license-name	Name of a specific license.

Command Default

None.

This example shows how to display the license details:

```
> show license detail wplus
Feature: wplus           Period left: Life time
Index:  1       Feature: wplus   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
        Store Index: 2
        Store Name: Primary License Storage
Index:  2       Feature: wplus   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  6 weeks  6 days
        License Count: Non-Counted
        License Priority: Low
        Store Index: 0
```

Related Commands

license install

show license agent

show license all

show license feature

show license image-level

show license summary

license modify priority

show license expiring

To display details of expiring licenses on the Cisco 5500 Series Controller, use the **show license expiring** command.

show license expiring

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the details of the expiring licenses:

```
> show license expiring
StoreIndex:  0  Feature: wplus   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  6 weeks  6 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  1  Feature: wplus-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  2 weeks  3 days
            Expiry date: Thu Jun 25 18:09:43 2009
        License Count: 250/250/0
        License Priority: High
StoreIndex:  2  Feature: base   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  4 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  3  Feature: base-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  3 days
        License Count: 250/0/0
        License Priority: Low
```

Related Commands

license install

show license all

show license detail

show license in-use

show license summary

license modify priority

show license evaluation

show license evaluation

To display details of evaluation licenses on the Cisco 5500 Series Controller, use the **show license evaluation** command.

show license evaluation

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the details of the evaluation licenses:

```
> show license evaluation
StoreIndex:  0  Feature: wplus   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  6 weeks  6 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  1  Feature: wplus-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  2 weeks  3 days
            Expiry date: Thu Jun 25 18:09:43 2009
        License Count: 250/250/0
        License Priority: High
StoreIndex:  2  Feature: base   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  4 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  3  Feature: base-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  3 days
        License Count: 250/0/0
        License Priority: Low
```

Related Commands

license install

show license all

show license detail

show license expiring

show license in-use

show license summary

license modify priority

show license feature

To display a summary of license-enabled features on the Cisco 5500 Series Controller, use the **show license feature** command.

show license feature

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the license-enabled features:

```
> show license feature
        Feature name Enforcement  Evaluation  Clear Allowed  Enabled
               wplus         yes         yes            yes      yes
      wplus-ap-count         yes         yes            yes      yes
                base          no         yes            yes       no
       base-ap-count         yes         yes            yes       no
```

Related Commands

license install

show license all

show license detail

show license expiring

show license image-level

show license in-use

show license summary

show license modify priority

show license evaluation

show license file

To display a summary of license-enabled features on the Cisco 5500 Series Controller, use the **show license file** command.

show license file

Syntax Description

This command has no arguments or keywords.

This example shows how to display the license files:

```
> show license file
License Store: Primary License Storage
  Store Index: 0
    License: 11 wplus-ap-count 1.0 LONG NORMAL STANDALONE EXCL 12_KEYS INFINIT
             E_KEYS NEVER NEVER NiL SLM_CODE CL_ND_LCK NiL *1AR5NS7M5AD8PPU400
              NiL NiL NiL 5_MINS <UDI><PID>AIR-CT5508-K9</PID><SN>RFD000P2D27<
             /SN></UDI> Pe0L7tv8KDUqo:zlPe423S5wasgM8G,tTs0i,7zLyA3VfxhnIe5aJa
             m63lR5l8JM3DPkr4O2DI43iLlKn7jomo3RFl1LjMRqLkKhiLJ2tOyuftQSq2bCAO6
             nR3wIb38xKi3t$<WLC>AQEBIQAB//++mCzRUbOhw28vz0czAY0iAm7ocDLUMb9ER0
             +BD3w2PhNEYwsBN/T3xXBqJqfC+oKRqwInXo3s+nsLU7rOtdOxoIxYZAo3LYmUJ+M
             FzsqlhKoJVlPyEvQ8H21MNUjVbhoN0gyIWsyiJaM8AQIkVBQFzhr10GYolVzdzfJf
             EPQIx6tZ++/Vtc/q3SF/5Ko8XCY=</WLC>
    Comment:
       Hash: iOGjuLlXgLhcTB113ohIzxVioHA=
. . .
```

Related Commands

license install

show license all

show license detail

show license expiring

show license feature

show license image-level

show license in-use

show license summary

show license evaluation

show license handle

To display the license handles on the Cisco 5500 Series Controller, use the **show license handle** command.

show license handle

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the license handles:

```
> show license handle
Feature: wplus                          , Handle Count: 1
    Units: 01( 0), ID: 0x5e000001, NotifyPC: 0x1001e8f4 LS-Handle (0x00000001),
Units: ( 1)
    Registered clients: 1
        Context 0x1051b610, epID 0x10029378
Feature: base                           , Handle Count: 0
    Registered clients: 1
        Context 0x1053ace0, epID 0x10029378
Feature: wplus-ap-count                 , Handle Count: 1
    Units: 250( 0), ID: 0xd4000002, NotifyPC: 0x1001e8f4        LS-Handle (0x000
00002), Units: (250)
    Registered clients: None
Feature: base-ap-count                  , Handle Count: 0
    Registered clients: None
Global Registered clients: 2
               Context 0x10546270, epID 0x100294cc
               Context 0x1053bae8, epID 0x100294cc
```

Related Commands

license install

show license all

show license detail

show license expiring

show license feature

show license image-level

show license in-use

show license summary

show license image-level

To display the license image level that is in use on the Cisco 5500 Series Controller, use the **show license image-level** command.

show license image-level

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the image level license settings:

```
> show license image-level
Module name  Image level  Priority  Configured  Valid license
wnbu         wplus        1         YES         wplus
             base         2         NO
 NOTE: wplus includes two additional features: Office Extend AP, Mesh AP.
```

Related Commands

license install

show license all

show license detail

show license expiring

show license feature

license modify priority

show license in-use

show license summary

show license in-use

To display the licenses that are in use on the Cisco 5500 Series Controller, use the **show license in-use** command.

show license in-use

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the licenses that are in use:

```
> show license in-use
StoreIndex:  2  Feature: wplus   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
StoreIndex:  1  Feature: wplus-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  2 weeks  3 days
            Expiry date: Thu Jun 25 18:09:43 2009
        License Count: 250/250/0
        License Priority: High
```

Related Commands

license install

show license all

show license detail

show license expiring

show license feature

show license image-level

show license modify priority

show license summary

show license permanent

show license evaluation

show license permanent

To display the permanent licenses on the Cisco 5500 Series Controller, use the **show license permanent** command.

show license permanent

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the permanent license's information:

```
> show license permanent
StoreIndex:  0  Feature: wplus-ap-count   Version: 1.0
        License Type: Permanent
        License State: Inactive
        License Count: 12/0/0
        License Priority: Medium
StoreIndex:  1  Feature: base   Version: 1.0
        License Type: Permanent
        License State: Active, Not in Use
        License Count: Non-Counted
        License Priority: Medium
StoreIndex:  2  Feature: wplus   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
```

Related Commands

license install

show license all

show license detail

show license expiring

show license feature

show license image-level

show license in-use

show license summary

license modify priority

show license evaluation

show license status

To display the license status on the Cisco Wireless Controller, use the **show license status** command.

show license status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to view the **license status** on the RTU license mechanism:

```
> show license status
               License Type Supported
       permanent  Non-expiring node locked license
       extension  Expiring node locked license
       evaluation Expiring non node locked license
               License Operation Supported
       install    Install license
       clear      Clear license
       annotate   Comment license
       save       Save license
       revoke     Revoke license
               Device status
       Device Credential type: DEVICE
       Device Credential Verification: PASS
       Rehost Type: DC_OR_IC
```

show license statistics

To display license statistics on the Cisco 5500 Series Controller, use the **show license statistics** command.

show license statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the license statistics:

```
> show license statistics
                Administrative statistics
        Install success count:       0
        Install failure count:       0
        Install duplicate count:     0
        Comment add count:           0
        Comment delete count:        0
        Clear count:                 0
c        Save count:                  0
        Save cred count:             0
                Client status
        Request success count     2
        Request failure count     0
        Release count             0
        Global Notify count       0
```

Related Commands

license install

show license all

show license detail

show license expiring

show license feature

show license image-level

show license in-use

show license summary

license modify priority

show license evaluation

show license summary

To display a brief summary of all licenses on the Cisco WLCs, use the **show license summary** command.

show license summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display a brief summary of all licenses:

```
> show license summary
Index 1 Feature: wplus
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: wplus-ap-count
        Period left:  2 weeks  3 days
        License Type: Evaluation
        License State: Active, In Use
        License Count: 250/250/0
        License Priority: High
Index 3 Feature: base
        Period left: Life time
        License Type: Permanent
        License State: Active, Not in Use
        License Count: Non-Counted
        License Priority: Medium
Index 4 Feature: base-ap-count
        Period left:  8 weeks  3 days
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
        License Count: 250/0/0
        License Priority: Low
```

show license udi

To display unique device identifier (UDI) values for licenses on the Cisco WLCs, use the **show license udi** command.

show license udi

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to view the UDI values for licenses on the RTU license mechanism:

```
(Cisco Controller) > show license udi
Device# PID                   SN                    UDI
------------------------------------------------------------------------------
*0      AIR-CT5508-K9         RFD000P2D27           AIR-CT5508-K9:RFD000P2D27
```

show load-balancing

To display the status of the load-balancing feature, use the **show load-balancing** command.

show load-balancing

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the load-balancing status:

```
> show load-balancing
Aggressive Load Balancing..................... Enabled
Aggressive Load Balancing Window.............. 0 clients
Aggressive Load Balancing Denial Count........... 3
Statistics
Total Denied Count............................ 10 clients
Total Denial Sent............................. 20 messages
Exceeded Denial Max Limit Count............... 0 times
None 5G Candidate Count....................... 0 times
None 2.4G Candidate Count..................... 0 times
```

Related Commands

config load-balancing

show local-auth certificates

To display local authentication certificate information, use the **show local-auth certificates** command:

show local-auth certificates

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to display the authentication certificate information stored locally:

```
(Cisco Controller) > show local-auth certificates
```

Related Commands

clear stats local-auth

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth config

show local-auth statistics

show logging

To display the syslog facility logging parameters and buffer contents, use the **show logging** command.

show logging

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to display the current settings and buffer content details:

```
(Cisco Controller) >show logging

(Cisco Controller) > config logging syslog host 10.92.125.52
System logs will be sent to 10.92.125.52 from now on

(Cisco Controller) > config logging syslog host 2001:9:6:40::623
System logs will be sent to 2001:9:6:40::623 from now on

(Cisco Controller) > show logging
Logging to buffer :
- Logging of system messages to buffer :
 - Logging filter level.......................... errors
 - Number of system messages logged.............. 1316
 - Number of system messages dropped............. 6892
- Logging of debug messages to buffer ........... Disabled
 - Number of debug messages logged............... 0
 - Number of debug messages dropped.............. 0
- Cache of logging  ............................. Disabled
- Cache of logging time(mins) ................... 10080
- Number of over cache time log dropped  ........ 0
Logging to console :
- Logging of system messages to console :
 - Logging filter level.......................... disabled
 - Number of system messages logged.............. 0
 - Number of system messages dropped............. 8243
- Logging of debug messages to console .......... Enabled
 - Number of debug messages logged............... 0
 - Number of debug messages dropped.............. 0
Logging to syslog :
- Syslog facility................................ local0
- Logging of system messages to console :
 - Logging filter level.......................... disabled
 - Number of system messages logged.............. 0
 - Number of system messages dropped............. 8208
- Logging of debug messages to console .......... Enabled
 - Number of debug messages logged............... 0
 - Number of debug messages dropped.............. 0
- Logging of system messages to syslog :
 - Logging filter level.......................... errors
 - Number of system messages logged.............. 1316
 - Number of system messages dropped............. 6892
```

```
- Logging of debug messages to syslog ..... Disabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Number of remote syslog hosts..... 2
- syslog over tls..... Disabled
  - Host 0..... 10.92.125.52
  - Host 1..... 2001:9:6:40::623
  - Host 2.....
Logging of RFC 5424..... Disabled
Logging of Debug messages to file :
- Logging of Debug messages to file..... Disabled
- Number of debug messages logged..... 0
- Number of debug messages dropped..... 0
Logging of traceback..... Enabled
```

show logging flags

To display the existing flags, use the **show logging flags** command.

show logging flags *AP* | *Cilent*

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the current flags details:

```
> show logging flags
ID    username     Connection From   Idle Time    Login Time
-- ---------------  ---------------  ------------  ------------
00 admin            EIA-232          00:00:00      00:19:04
```

Related Commands

config logging flags close

show loginsession

To display the existing sessions, use the **show loginsession** command.

show loginsession

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the current session details:

```
> show loginsession
ID    username     Connection From   Idle Time    Session Time
-- ---------------  ---------------  ------------  ------------
00 admin            EIA-232          00:00:00      00:19:04
```

Related Commands

config loginsession close

show mesh cac

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

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

Syntax Description

summary	Displays the total number of voice calls and voice bandwidth used for each mesh access point.
bwused	Displays the bandwidth for a selected access point in a tree topology.
voice	Displays the mesh topology and the voice bandwidth used or available.
video	Displays the mesh topology and the video bandwidth used or available.
access	Displays access voice calls in progress in a tree topology.
callpath	Displays the call bandwidth distributed across the mesh tree.
rejected	Displays voice calls rejected for insufficient bandwidth in a tree topology.
cisco_ap	Mesh access point name.

Command Default

None

Command History

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

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

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

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

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

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

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

show mdns profile

To display mDNS profile information, use the **show mdns profile** command.

show mdns profile {**summary** | **detailed** *profile-name*}

Syntax Description

summary	Displays the summary of the mDNS profiles.
detailed	Displays details of an mDNS profile.
profile-name	Name of the mDNS profile.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

This example shows how to display a summary of all the mDNS profiles:

```
> show mdns profile summary
Number of Profiles.............................. 2

ProfileName                       No. Of Services
--------------------------------  ---------------
default-mdns-profile                   5
profile1                               2
```

This example shows how to display the detailed information of an mDNS profile:

```
> show mdns profile detailed default-mdns-profile

Profile Name.................................... default-mdns-profile
Profile Id...................................... 1
No of Services.................................. 5
Services........................................ AirPrint
                                                 AppleTV
                                                 HP_Photosmart_Printer_1
                                                 HP_Photosmart_Printer_2
                                                 Printer

No. Interfaces Attached......................... 0
No. Interface Groups Attached................... 0
No. Wlans Attached.............................. 1
Wlan Ids........................................ 1
```

Related Commands

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

config mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

show mdns service

To display multicast Domain Name System (mDNS) service information, use the **show mnds service** command.

show mdns service { **summary** | **detailed** *service-name* }

Syntax Description

summary	Displays the summary of all mDNS services.
detailed	Displays the details of an mDNS service.
service-name	Name of the mDNS service.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show mnds summary** command:

```
Device > show mdns service summary

Number of Services.............................. 5

Service-Name               Service-string
------------------------
AirPrint                        _ipp._tcp.local.
AppleTV                         _airplay._tcp.local.
HP_Photosmart_Printer_1         _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2         _cups._sub._ipp._tcp.local.
Printer                         _printer._tcp.local.
```

The following is a sample output of the **show mnds service detailed** command:

```
Device > show mdns service detailed AirPrint

Service Name.................................... AirPrint
Service Id...................................... 1
Service query status............................ Enabled

Number of Profiles.............................. 2
Profile......................................... student-profile, guest-profile


Number of Service Providers ..................... 2

Service Provider MAC-Address       VLAN ID  Type
---------------- -----------       -------  ----
user1         60:33:4b:2b:a6:9a              104  Wired
laptopa       00:21:1b:ea:36:60   105  Wireless
```

The following is a sample output of the **show mnds service not-learnt**command:

Related Topics

config wlan mdns
config mdns profile, on page 179
config mdns query interval, on page 181
config mdns service , on page 182
config mdns snooping , on page 183
clear mdns service-database, on page 26
debug mdns all, on page 506
debug mdns detail , on page 507
debug mdns error , on page 507
debug mdns message , on page 508
show mdns profile, on page 427

show mgmtuser

To display the local management user accounts on the Cisco wireless LAN controller, use the **show mgmtuser** command.

show mgmtuser

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display a list of management users:

```
> show mgmtuser
User Name                 Permissions    Description            Password Strength
-----------------------   ------------   --------------         ------------------
admin                     read-write                                    Weak
```

Related Commands

config mgmtuser add

config mgmtuser delete

config mgmtuser description

config mgmtuser password

show mobility group member

To display the details of the mobility group members in the same domain, use the **show mobility group member** command.

show mobility group member hash

Syntax Description

hash	Displays the hash keys of the mobility group members in the same domain.

Command Default

None

Command History

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

The following example shows how to display the hash keys of the mobility group members:

```
(Cisco Controller) >show mobility group member hash
Default Mobility Domain..................... new-mob

 IP Address      Hash Key
-------------------------------------------------------

 9.2.115.68      a819d479dcfeb3e0974421b6e8335582263d9169

 9.6.99.10       0974421b6e8335582263d9169a819d479dcfeb3e

 9.7.7.7         feb3e0974421b6e8335582263d9169a819d479dc
```

show netuser

To display the configuration of a particular user in the local user database, use the **show netuser** command.

show netuser {**detail** *user_name* | **guest-roles** | **summary**}

Syntax Description

detail	Displays detailed information about the specified network user.
user_name	Network user.
guest_roles	Displays configured roles for guest users.
summary	Displays a summary of all users in the local user database.

Command Default

None

Command History

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

The following is a sample output of the **show netuser summary** command:

```
(Cisco Controller) > show netuser summary
Maximum logins allowed for a given username ........Unlimited
```

The following is a sample output of the **show netuser detail** command:

```
(Cisco Controller) > show netuser detail john10
username..................................... abc
WLAN Id...................................... Any
Lifetime..................................... Permanent
Description.................................. test user
```

Related Commands

config netuser add

config netuser delete

config netuser description

config netuser guest-role apply

config netuser wlan-id

config netuser guest-roles

show netuser guest-roles

To display a list of the current quality of service (QoS) roles and their bandwidth parameters, use the **show netuser guest-roles** command.

show netuser guest-roles

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

This example shows how to display a QoS role for the guest network user:

```
(Cisco Controller) > show netuser guest-roles
Role Name............................. Contractor
 Average Data Rate.................... 10
 Burst Data Rate...................... 10
 Average Realtime Rate................ 100
 Burst Realtime Rate.................. 100
Role Name............................. Vendor
 Average Data Rate.................... unconfigured
 Burst Data Rate...................... unconfigured
 Average Realtime Rate................ unconfigured
 Burst Realtime Rate.................. unconfigured
```

Related Commands

config netuser add

config netuser delete

config netuser description

config netuser guest-role apply

config netuser wlan-id

show netuser guest-roles

show netuser

show network

To display the current status of 802.3 bridging for all WLANs, use the **show network** command.

show network

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the network details:

```
(Cisco Controller) > show network
```

Related Commands

config network

show network summary

show network multicast mgid detail

show network multicast mgid summary

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.

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

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
oeap-600 dual-rlan-ports ................... Disable
```

```
oeap-600 local-network ..................... Enable
mDNS snooping............................... Disabled
mDNS Query Interval......................... 15 minutes

Web Color Theme............................. Default
CAPWAP Prefer Mode.......................... IPv4
```

show network multicast mgid detail

To display all the clients joined to the multicast group in a specific multicast group identification (MGID), use the **show network multicast mgid detail** command.

show network multicast mgid detail *mgid_value*

Syntax Description

mgid_value	Number between 550 and 4095.

Command Default

None.

This example shows how to display details of the multicast database:

```
> show network multicast mgid detail
Mgid ............................... 550
Multicast Group Address ............ 239.255.255.250
Vlan ............................... 0
Rx Packet Count .................... 807399588
No of clients ...................... 1
Client List .......................
  Client MAC       Expire TIme (mm:ss)
   00:13:02:23:82:ad   0:20
```

Related Commands

show network summary

show network multicast mgid detail

show network

show network multicast mgid summary

To display all the multicast groups and their corresponding multicast group identifications (MGIDs), use the **show network multicast mgid summary** command.

show network multicast mgid summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display a summary of multicast groups and their MGIDs:

```
> show network multicast mgid summary
Layer2 MGID Mapping:
--------------------
InterfaceName             vlanId     MGID
---------------------------- ------  -----
management              0       0
test             0    9
wired           20     8
Layer3 MGID Mapping:
--------------------
Number of Layer3 MGIDs ................. 1
 Group address          Vlan    MGID
 -----------------  -----   ------
 239.255.255.250        0      550
```

Related Commands

show network summary

show network multicast mgid detail

show network

show nmsp notify-interval summary

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmsp notify-interval summary** command.

show nmsp notify-interval summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display NMSP configuration settings:

```
> show nmsp notify-interval summary
NMSP Notification Interval Summary
 Client
        Measurement interval:    2 sec
 RFID
        Measurement interval:    8 sec
 Rogue AP
        Measurement interval:    2 sec
 Rogue Client
        Measurement interval:    2 sec
```

Related Commands

clear locp statistics

clear nmsp statistics

config nmsp notify-interval measurement

show nmsp statistics

show nmsp status

show nmsp statistics

To display Network Mobility Services Protocol (NMSP) counters, use the **show nmsp statistics** command.

show nmsp statistics {**summary** | **connection all**}

Syntax Description

summary	Displays common NMSP counters.
connection all	Displays all connection-specific counters.

Command Default

None.

This example shows how to display a summary of common NMSP counters:

```
> show nmsp statistics summary
Send RSSI with no entry:               0
Send too big msg:                      0
Failed SSL write:                      0
Partial SSL write:                     0
SSL write attempts to want write:
Transmit Q full:0
Max Measure Notify Msg:                0
Max Info Notify Msg:                   0
Max Tx Q Size:                         2
Max Rx Size:                           1
Max Info Notify Q Size:                0
Max Client Info Notify Delay:          0
Max Rogue AP Info Notify Delay:        0
Max Rogue Client Info Notify Delay:    0
Max Client Measure Notify Delay:       0
Max Tag Measure Notify Delay:          0
Max Rogue AP Measure Notify Delay:     0
Max Rogue Client Measure Notify Delay: 0
Max Client Stats Notify Delay:         0
Max Tag Stats Notify Delay:            0
RFID Measurement Periodic :            0
RFID Measurement Immediate :           0
Reconnect Before Conn Timeout:         0
```

This example shows how to display all the connection-specific NMSP counters:

```
> show nmsp statistics connection all
NMSP Connection Counters
Connection 1 :
 Connection status:  UP
 Freed Connection:    0
 Nmsp Subscr Req:     0          NMSP Subscr Resp:   0
 Info Req:            1          Info Resp:          1
 Measure Req:         2          Measure Resp:        2
 Stats Req:           2          Stats Resp:          2
 Info Notify:         0          Measure Notify:      0
 Loc Capability:      2
 Location Req:        0          Location Rsp:        0
 Loc Subscr Req:      0          Loc Subscr Rsp:      0
 Loc Notif:           0
 Loc Unsubscr Req:    0          Loc Unsubscr Rsp:    0
```

```
IDS Get Req:          0           IDS Get Resp:         0
IDS Notif:            0
IDS Set Req:          0           IDS Set Resp:         0
```

Related Commands

show nmsp notify-interval summary

clear nmsp statistics

config nmsp notify-interval measurement

show nmsp status

show nmsp status

To display the status of active Network Mobility Services Protocol (NMSP) connections, use the **show nmsp status** command.

show nmsp status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the status of the active NMSP connections:

```
> show nmsp status
LocServer IP   TxEchoResp  RxEchoReq TxData  RxData
-------------- ----------- --------- ------- -------
171.71.132.158 21642       21642     51278   21253
```

Related Commands

show nmsp notify-interval summary

clear nmsp statistics

config nmsp notify-interval measurement

show nmsp status

clear locp statistics

show nmsp statistics

show nmsp subscription

To display the Network Mobility Services Protocol (NMSP) services that are active on the controller, use the **show nmsp subscription** command.

show nmsp subscription {**summary** | **detail** *ip-addr*}

Syntax Description

summary	Displays all of the NMSP services to which the controller is subscribed.
detail	Displays details for all of the NMSP services to which the controller is subscribed.
ip-addr	Details only for the NMSP services subscribed to by a specific IPv4 or IPv6 address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

This example shows how to display a summary of all the NMSP services to which the controller is subscribed:

```
> show nmsp subscription summary
Mobility Services Subscribed:
Server IP          Services
---------          --------
10.10.10.31        RSSI, Info, Statistics
```

This example shows how to display details of all the NMSP services:

```
> show nmsp subscription detail 10.10.10.31
Mobility Services Subscribed by 10.10.10.31
Services          Sub-services
--------          ------------
RSSI              Mobile Station, Tags,
Info              Mobile Station,
Statistics        Mobile Station, Tags,

> show nmsp subscription detail 2001:9:6:40::623
Mobility Services Subscribed by 2001:9:6:40::623
Services          Sub-services
--------          ------------
RSSI              Mobile Station, Tags,
Info              Mobile Station,
Statistics        Mobile Station, Tags,
```

Related Topics

show nmsp notify-interval summary, on page 440
show nmsp statistics, on page 441
config nmsp notify-interval measurement, on page 253
clear nmsp statistics, on page 27
clear locp statistics, on page 23

show ntp-keys

To display network time protocol authentication key details, use the **show ntp-keys** command.

show ntp-keys

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

This example shows how to display NTP authentication key details:

```
(Cisco Controller) > show ntp-keys
Ntp Authentication Key Details...................
      Key Index
     -----------
         1
         3
```

Related Commands

config time ntp

show qos

To display quality of service (QoS) information, use the **show qos** command.

show qos {**bronze** | **gold** | **platinum** | **silver**}

Syntax Description

bronze	Displays QoS information for the bronze profile of the WLAN.
gold	Displays QoS information for the gold profile of the WLAN.
platinum	Displays QoS information for the platinum profile of the WLAN.
silver	Displays QoS information for the silver profile of the WLAN.

Command Default

None.

This example shows how to display QoS information for the gold profile:

```
> show qos gold
Description..................................... For Video Applications
Maximum Priority................................ video
Unicast Default Priority........................ video
Multicast Default Priority...................... video
Per-SSID Rate Limits............................ UpstreamDownstream
Average Data Rate............................... 0 0
Average Realtime Data Rate...................... 0 0
Burst Data Rate................................. 0 0
Burst Realtime Data Rate........................ 0 0
Per-Client Rate Limits.......................... UpstreamDownstream
Average Data Rate............................... 0 0
Average Realtime Data Rate...................... 0 0
Burst Data Rate................................. 0 0
Burst Realtime Data Rate........................ 0 0
protocol........................................ none

802.11a Customized EDCA Settings:
ecwmin.......................................... 3
ecwmax.......................................... 4
aifs............................................ 7
txop............................................ 94

802.11a Customized packet parameter Settings:
Packet retry time............................... 3
Not retrying threshold.......................... 100
Disassociating threshold........................ 500
Time out value.................................. 35
```

Related Commands

config qos protocol-type

show reset

To display the scheduled system reset parameters, use the **show reset** command.

show reset

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the scheduled system reset parameters:

```
> show reset
System reset is scheduled for Mar 27 01 :01 :01 2010
Current local time and date is Mar 24 02:57:44 2010
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel the reset.
Configuration will be saved before the system reset.
```

Related Commands

reset system at

reset system in

reset system cancel

reset system notify-time

show route kernel

To display the kernel route cache information, use the **show route kernel** command.

show route kernel

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the kernel route cache information:

```
> show route kernel
Iface  Destination  Gateway   Flags    RefCnt Use  Metric   Mask   MTU   Window   IRTT
dtl0    14010100    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    28282800    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    34010100    00000000  0001      0     0     0    FFFFFF00  0      0        0
eth0    02020200    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    33010100    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    0A010100    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    32010100    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    0A000000    0202020A  0003      0     0     0    FF000000  0      0        0
lo      7F000000    00000000  0001      0     0     0    FF000000  0      0        0
dtl0    00000000    0A010109  0003      0     0     0    00000000  0      0        0
```

Related Commands

clear ap

debug arp

show arp kernel

config route add

config route delete

show route summary

To display the routes assigned to the Cisco wireless LAN controller service port, use the **show route summary** command.

show route summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display all the configured routes:

```
> show route summary
Number of Routes.............................. 1
Destination Network          Genmask              Gateway
-------------------    -------------------   -------------------
xxx.xxx.xxx.xxx        255.255.255.0         xxx.xxx.xxx.xxx
```

Related Commands

config route

show sessions

To display the console port login timeout and maximum number of simultaneous command-line interface (CLI) sessions, use the **show sessions** command.

show sessions

Syntax Description

This command has no arguments or keywords.

Command Default

5 minutes, 5 sessions.

This example shows how to display the CLI session configuration setting:

```
> show sessions
CLI Login Timeout (minutes)..... 0
Maximum Number of CLI Sessions..... 5
```

The response indicates that the CLI sessions never time out and that the Cisco wireless LAN controller can host up to five simultaneous CLI sessions.

Related Commands

config sessions maxsessions

config sessions timeout

show snmpcommunity

To display Simple Network Management Protocol (SNMP) community entries, use the **show snmpcommunity** command.

show snmpcommunity

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display SNMP community entries:

```
> show snmpcommunity
SNMP Community Name Client IP Address Client IP Mask    Access Mode Status
------------------- ----------------- ----------------- ----------- --------
public              0.0.0.0           0.0.0.0           Read Only   Enable
**********          0.0.0.0           0.0.0.0           Read/Write  Enable
```

Related Commands

config snmp community accessmode

config snmp community create

config snmp community delete

config snmp community ipaddr

config snmp community mode

config snmp syscontact

show snmpengineID

To display the SNMP engine ID, use the **show snmpengineID** command.

show snmpengineID

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the SNMP engine ID:

```
> show snmpengineID
SNMP EngineId... ffffffffffff
```

Related Commands

config snmp engineID

show snmptrap

To display Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap receivers and their status, use the **show snmptrap** command.

show snmptrap

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display SNMP trap receivers and their status:

```
> show snmptrap
SNMP Trap Receiver Name    IP Address        Status
-------------------------  ----------------- --------
xxx.xxx.xxx.xxx            xxx.xxx.xxx.xxx   Enable
```

show snmpv3user

To display Simple Network Management Protocol (SNMP) version 3 configuration, use the **show snmpv3user** command.

show snmpv3user

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display SNMP version 3 configuration information:

```
> show snmpv3user
SNMP v3 username    AccessMode  Authentication Encryption
------------------- ----------- -------------- ----------
default              Read/Write  HMAC-SHA       CFB-AES
```

Related Commands

config snmp v3user create

config snmp v3user delete

show snmpversion

To display which versions of Simple Network Management Protocol (SNMP) are enabled or disabled on your controller, use the **show snmpversion** command.

show snmpversion

Syntax Description

This command has no arguments or keywords.

Command Default

Enable.

This example shows how to display the SNMP v1/v2/v3 status:

```
> show snmpversion
SNMP v1  Mode..................................... Disable
SNMP v2c Mode..................................... Enable
SNMP v3  Mode..................................... Enable
```

Related Commands

config snmp version

show switchconfig

To display parameters that apply to the Cisco wireless LAN controller, use the **show switchconfig** command.

show switchconfig

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command History

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

This example shows how to display parameters that apply to the Cisco wireless LAN controller:

```
(Cisco Controller) >> show switchconfig
802.3x Flow Control Mode..................... Disabled
FIPS prerequisite features................... Enabled
Boot Break................................... Enabled
secret obfuscation........................... Enabled
Strong Password Check Features:
         case-check ...........Disabled
         consecutive-check ....Disabled
         default-check .......Disabled
         username-check ......Disabled
```

Related Commands

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig strong-pwd

config switchconfig flowcontrol

config switchconfig fips-prerequisite

show stats switch

show sysinfo

To display high-level Cisco WLC information, use the **show sysinfo** command.

show sysinfo

Syntax Description

This command has no arguments or keywords.

Command Default

None

This example shows a sample output of the command run on Cisco 8540 Wireless Controller using Release 8.3:

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.3.100.0
RTOS Version..................................... 8.3.100.0
Bootloader Version............................... 8.0.110.0
Emergency Image Version.......................... 8.0.110.0

OUI File Last Update Time........................ Sun Sep 07 10:44:07 IST 2014


Build Type....................................... DATA + WPS

System Name...................................... TestSpartan8500Dev1
System Location..................................
System Contact...................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.1615
Redundancy Mode.................................. Disabled
IP Address....................................... 8.1.4.2
IPv6 Address..................................... ::
System Up Time................................... 0 days 17 hrs 20 mins 58 secs

--More-- or (q)uit
System Timezone Location.........................
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... Multiple Countries : IN,US
Operating Environment............................ Commercial (10 to 35 C)
Internal Temp Alarm Limits....................... 10 to 38 C
Internal Temperature............................. +21 C
Fan Status....................................... OK

RAID Volume Status
Drive 0.......................................... Good
Drive 1.......................................... Good

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
Number of WLANs.................................. 7
Number of Active Clients......................... 1

OUI Classification Failure Count................. 0
```

```
Burned-in MAC Address.......................... F4:CF:E2:0A:27:00
Power Supply 1................................. Present, OK

--More-- or (q)uit
Power Supply 2................................. Present, OK
Maximum number of APs supported................ 6000
System Nas-Id..................................
WLC MIC Certificate Types...................... SHA1/SHA2
Licensing Type................................. RTU
```

show tech-support

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support** command.

show tech-support

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display system resource information:

```
> show tech-support
Current CPU Load..................................... 0%
System Buffers
   Max Free Buffers.................................. 4608
   Free Buffers...................................... 4604
   Buffers In Use.................................... 4
Web Server Resources
   Descriptors Allocated............................. 152
   Descriptors Used.................................. 3
   Segments Allocated................................ 152
   Segments Used..................................... 3
System Resources
   Uptime............................................ 747040 Secs
   Total Ram......................................... 127552 Kbytes
   Free Ram.......................................... 19540 Kbytes
   Shared Ram........................................ 0 Kbytes
   Buffer Ram........................................ 460 Kbytes
```

show time

To display the Cisco wireless LAN controller time and date, use the **show time** command.

show time

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the controller time and date when authentication is not enabled:

```
> show time
Time..................................... Wed Apr 13 09:29:15 2011
Timezone delta........................... 0:0
Timezone location........................ (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
NTP Servers
    NTP Polling Interval.....................     3600
     Index     NTP Key Index     NTP Server      NTP Msg Auth Status
    -------  ------------------------------------------------------------
       1              0           9.2.60.60       AUTH DISABLED
```

This example shows successful authentication of NTP Message results in the AUTH Success:

```
> show time
Time..................................... Thu Apr  7 13:56:37 2011
Timezone delta........................... 0:0
Timezone location........................ (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
NTP Servers
    NTP Polling Interval.....................     3600
     Index     NTP Key Index     NTP Server      NTP Msg Auth Status
    -------  ------------------------------------------------------------
       1              1           9.2.60.60       AUTH SUCCESS
```

This example shows that if the packet received has errors, then the NTP Msg Auth status will show AUTH Failure:

```
> show time
Time..................................... Thu Apr  7 13:56:37 2011
Timezone delta........................... 0:0
Timezone location........................ (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
NTP Servers
    NTP Polling Interval.....................     3600
     Index     NTP Key Index     NTP Server      NTP Msg Auth Status
    -------  ------------------------------------------------------------
       1              10           9.2.60.60       AUTH FAILURE
```

This example shows that if there is no response from NTP server for the packets, the NTP Msg Auth status will be blank:

```
> show time
Time..................................... Thu Apr  7 13:56:37 2011
Timezone delta........................... 0:0
Timezone location........................ (GMT +5:30) Colombo, New Delhi, Chennai,
 Kolkata
```

```
NTP Servers
    NTP Polling Interval.........................     3600
     Index     NTP Key Index     NTP Server      NTP Msg Auth Status
    -------  ------------------------------------------------------------
       1              11           9.2.60.60
```

Related Commands

config time manual

config time ntp

config time timezone

config time timezone location

show trapflags

To display the Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap flags, use the **show trapflags** command.

show trapflags

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display controller SNMP trap flags:

```
> show trapflags
Authentication Flag.......................... Enable
Link Up/Down Flag............................ Enable
Multiple Users Flag.......................... Enable
Spanning Tree Flag........................... Enable
Client Related Traps
        802.11 Disassociation..................... Disable
        802.11 Association.........................Disabled
        802.11 Deauthenticate..................... Disable
        802.11 Authenticate Failure............... Disable
        802.11 Association Failure................ Disable
        Authentication.............................Disabled
        Excluded.................................. Disable
        Max Client Warning Threshold.............. 90%
       Nac-Alert Traps............................... Disabled
       RFID Related Traps
        Max RFIDs Warning Threshold..................... 90%

802.11 Security related traps
        WEP Decrypt Error......................... Enable
        IDS Signature Attack........................... Disable

Cisco AP
        Register.................................. Enable
        InterfaceUp............................... Enable
Auto-RF Profiles
        Load...................................... Enable
        Noise..................................... Enable
        Interference.............................. Enable
        Coverage.................................. Enable
Auto-RF Thresholds
        tx-power.................................. Enable
        channel................................... Enable
        antenna................................... Enable
AAA
        auth...................................... Enable
        servers................................... Enable
rogueap...................................... Enable
adjchannel-rogueap............................... Disabled
wps.......................................... Enable
configsave................................... Enable
IP Security
        esp-auth.................................. Enable
        esp-replay................................ Enable
        invalidSPI................................ Enable
```

```
        ike-neg..................................... Enable
        suite-neg................................... Enable
        invalid-cookie.............................. Enable
Mesh
        auth failure................................ Enabled
        child excluded parent....................... Enabled
        parent change............................... Enabled
        child moved................................. Enabled
        excessive parent change..................... Enabled
        onset SNR................................... Enabled
        abate SNR................................... Enabled
        console login............................... Enabled
        excessive association....................... Enabled
        default bridge group name................... Enabled
        excessive hop count......................... Disabled
        excessive children.......................... Enabled
        sec backhaul change......................... Disabled
```

Related Commands

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

show traplog

To display the Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap log, use the **show traplog** command.

show traplog

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following is a sample output of the **show traplog** command:

```
(Cisco Controller) > show traplog
Number of Traps Since Last Reset..... 2447
Number of Traps Since Log Last Displayed... 2447
Log System Time              Trap
--- ------------------------ ------------------------------------------------
  0 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:52:62:fe detected on Base Rad
                             io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
                             b/g) with RSSI: -78 and SNR: 10
  1 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:52:19:d8 detected on Base Rad
                             io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
                             b/g) with RSSI: -72 and SNR: 16
  2 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:26:a1:8d detected on Base Rad
                             io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
                             b/g) with RSSI: -82 and SNR: 6
  3 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:14:b3:4f detected on Base Rad
                             io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
                             b/g) with RSSI: -56 and SNR: 30
Would you like to display more entries? (y/n)
```

show rfid client

To display the radio frequency identification (RFID) tags that are associated to the controller as clients, use the **show rfid client** command.

show rfid client

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Usage Guidelines

When the RFID tag is not in client mode, the above fields are blank.

This example shows how to display the RFID tag that is associated to the controller as clients:

```
> show rfid client
------------------  -------- --------- ----------------- ------ ----------------
                                    Heard
   RFID Mac              VENDOR   Sec Ago    Associated AP    Chnl    Client State
------------------  -------- --------- ----------------- ------ ----------------
00:14:7e:00:0b:b1     Pango           35      AP0019.e75c.fef4     1          Probing
```

Related Commands

config rfid status

config rfid timeout

show rfid config

show rfid detail

show rfid summary

show rfid config

To display the current radio frequency identification (RFID) configuration settings, use the **show rfid config** command.

show rfid config

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the current RFID configuration settings:

```
> show rfid config
RFID Tag Data Collection ............................. Enabled
RFID Tag Auto-Timeout ................................ Enabled
RFID Client Data Collection ........................... Disabled
RFID Data Timeout ..................................... 200 seconds
```

Related Commands

config rfid status

config rfid timeout

show rfid client

show rfid detail

show rfid summary

show rfid detail

To display detailed radio frequency identification (RFID) information for a specified tag, use the **show rfid detail** command.

show rfid detail *mac_address*

Syntax Description

mac_address	MAC address of an RFID tag.

Command Default

None.

This example shows how to display detailed RFID information:

```
> show rfid detail 00:12:b8:00:20:52
RFID address..................................... 00:12:b8:00:20:52
Vendor........................................... G2
Last Heard....................................... 51 seconds ago
Packets Received................................. 2
Bytes Received................................... 324
Cisco Type.....................................
Content Header
=================
Version.......................................... 0
Tx Power......................................... 12 dBm
Channel.......................................... 1
Reg Class........................................ 12
Burst Length..................................... 1
CCX Payload
===========
Last Sequence Control............................ 0
Payload length................................... 127
Last Sequence Control............................ 0
Payload length................................... 127
Payload Data Hex Dump
01 09 00 00 00 00 0b 85 52 52 52 02 07 4b ff ff
7f ff ff ff 03 14 00 12 7b 10 48 53 c1 f7 51 4b
50 ba 5b 97 27 80 00 67 00 01 03 05 01 42 34 00
00 03 05 02 42 5c 00 00 03 05 03 42 82 00 00 03
05 04 42 96 00 00 03 05 05 00 00 00 55 03 05 06
42 be 00 00 03 02 07 05 03 12 08 10 00 01 02 03
04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 03 0d 09 03
08 05 07 a8 02 00 10 00 23 b2 4e 03 02 0a 03
Nearby AP Statistics:
lap1242-2(slot 0, chan 1) 50 seconds ag.... -76 dBm
lap1242(slot 0, chan 1) 50 seconds ago..... -65 dBm
```

Related Commands

config rfid status

config rfid timeout

show rfid config

show rfid client

show rfid summary

show rfid summary

To display a summary of the radio frequency identification (RFID) information for a specified tag, use the **show rfid summary** command.

show rfid summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display a summary of RFID information:

```
> show rfid summary
Total Number of RFID   : 5
----------------- -------- ------------------ ------ --------------------
     RFID ID      VENDOR       Closest AP      RSSI  Time Since Last Heard
----------------- -------- ------------------ ------ --------------------
00:04:f1:00:00:04 Wherenet ap:1120             -51      858 seconds ago
00:0c:cc:5c:06:d3 Aerosct  ap:1120             -51       68 seconds ago
00:0c:cc:5c:08:45 Aerosct  AP_1130             -54      477 seconds ago
00:0c:cc:5c:08:4b Aerosct  wolverine           -54      332 seconds ago
00:0c:cc:5c:08:52 Aerosct  ap:1120             -51      699 seconds ago
```

Related Commands

config rfid status

config rfid timeout

show rfid client

show rfid detail

show rfid config

Uploading and Downloading Files and Configurations

transfer download certpasswor

To set the password for the .PEM file so that the operating system can decrypt the web administration SSL key and certificate, use the **transfer download certpassword** command.

transfer download certpassword *private_key_password*

Syntax Description

private_key_password	Certificate's private key password.

Command Default

None

Command History

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

The following example shows how to transfer a file to the switch with the certificate's private key password certpassword:

```
(Cisco Controller) > transfer download certpassword
Clearing password
```

Related Topics

clear transfer, on page 38
transfer download mode, on page 472
transfer download filename, on page 472
transfer download path, on page 474
transfer download serverip, on page 475
transfer download start, on page 476
transfer upload datatype, on page 479
transfer upload mode, on page 482
transfer upload filename, on page 481
transfer upload path, on page 484
transfer upload serverip, on page 486
transfer upload start, on page 486

transfer download datatype

To set the download file type, use the **transfer download datatype** command.

transfer download datatype {**code** | **config** | **eapdevcert** | **eapcacert** | **icon** | **image** | **ipseccacert** | **ipsecdevcert** | **login-banner** | **signature** | **webadmincert** | **webauthbundle** | **webauthcert**}

Syntax Description

code	Downloads an executable image to the system.
config	Downloads the configuration file.
eapcacert	Downloads an EAP ca certificate to the system.
eapdevcert	Downloads an EAP dev certificate to the system.
icon	Downloads an executable image to the system.
image	Downloads a web page login to the system.
ipseccacert	Downloads an IPSec Certificate Authority (CA) certificate to the system.
ipsecdevcert	Downloads an IPSec dev certificate to the system.
login-banner	Downloads the controller login banner. Only text file is supported with a maximum of 1500 bytes.
signature	Downloads a signature file to the system.
webadmincert	Downloads a certificate for web administration to the system.
webauthbundle	Downloads a custom webauth bundle to the system.
webauthcert	Downloads a web certificate for the web portal to the system.

Command Default

None

Command History

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

The following example shows how to download an executable image to the system:

```
(Cisco Controller) > transfer download datatype code
```

Related Topics

clear transfer, on page 38
transfer download mode, on page 472
transfer download path, on page 474
transfer download serverip, on page 475
transfer download start, on page 476
transfer upload datatype, on page 479
transfer upload mode, on page 482
transfer upload filename, on page 481
transfer upload path, on page 484

transfer upload serverip, on page 486
transfer upload start, on page 486

transfer download filename

To download a specific file, use the **transfer download filename** command.

transfer download filename *filename*

Syntax Description		
	filename	Filename that contains up to 512 alphanumeric characters.

Command Default None

Command History

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

Usage Guidelines You cannot use special characters such as \ : * ? " < > | for the filename.

The following example shows how to transfer a file named build603:

```
(Cisco Controller) > transfer download filename build603
```

Related Topics

clear transfer, on page 38
transfer download certpasswor, on page 470
transfer download mode, on page 472
transfer download path, on page 474
transfer download serverip, on page 475
transfer download start, on page 476
transfer upload datatype, on page 479
transfer upload mode, on page 482
transfer upload filename, on page 481
transfer upload path, on page 484
transfer upload serverip, on page 486
transfer upload start, on page 486

transfer download mode

To set the transfer mode, use the **transfer download mode** command.

transfer upload mode {**ftp** | **tftp** | **sftp**}

Syntax Description		
	ftp	Sets the transfer mode to FTP.
	tftp	Sets the transfer mode to TFTP.

sftp	Sets the transfer mode to SFTP.

Command Default None

Command History

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

The following example shows how to transfer a file using the TFTP mode:

```
(Cisco Controller) > transfer download mode tftp
```

Related Topics

clear transfer, on page 38
transfer download filename, on page 472
transfer download certpasswor, on page 470
transfer download path, on page 474
transfer download serverip, on page 475
transfer download start, on page 476
transfer upload datatype, on page 479
transfer upload filename, on page 481
transfer upload path, on page 484
transfer upload serverip, on page 486
transfer upload start, on page 486

transfer download password

To set the password for an FTP transfer, use the **transfer download password** command.

transfer download password *password*

Syntax Description

password	Password.

Command Default None

Command History

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

The following example shows how to set the password for FTP transfer to pass01:

```
(Cisco Controller) > transfer download password pass01
```

Related Topics

transfer download mode, on page 472
transfer download port, on page 474

transfer upload username, on page 487

transfer download path

To set a specific FTP or TFTP path, use the **transfer download path** command.

transfer download path *path*

Syntax Description

path	Directory path. **Note** Path names on a TFTP or FTP server are relative to the server's default or root directory. For example, in the case of the Solarwinds TFTP server, the path is "/".

Command Default

None

Command History

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

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the file path.

The following example shows how to transfer a file to the path c:\install\version2:

```
(Cisco Controller) > transfer download path c:\install\version2
```

Related Topics

clear transfer, on page 38
transfer download mode, on page 472
transfer download certpasswor, on page 470
transfer download filename, on page 472
transfer download serverip, on page 475
transfer download start, on page 476
transfer upload datatype, on page 479
transfer upload mode, on page 482
transfer upload filename, on page 481
transfer upload path, on page 484
transfer upload serverip, on page 486
transfer upload start, on page 486

transfer download port

To specify the FTP port, use the **transfer download port** command.

transfer download port *port*

Syntax Description		
	port	FTP port.

Command Default The default FTP *port* is 21.

Command History

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

ch

The following example shows how to specify FTP port number 23:

```
(Cisco Controller) > transfer download port 23
```

Related Topics

transfer download mode, on page 472
transfer download path, on page 474
transfer download username, on page 478

transfer download serverip

To configure the IPv4 or IPv6 address of the TFTP server from which to download information, use the **transfer download serverip** command.

transfer download serverip *IP addr*

Syntax Description		
	IP addr	TFTP server IPv4 or IPv6 address.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure the IPv4 address of the TFTP server:

```
(Cisco Controller) > transfer download serverip 175.34.56.78
```

The following example shows how to configure the IPv6 address of the TFTP server:

```
(Cisco Controller) > transfer download serverip 2001:10:1:1::1
```

Related Topics

clear transfer, on page 38
transfer download mode, on page 472
transfer download filename, on page 472

transfer download path, on page 474
transfer download serverip, on page 475
transfer download start, on page 476
transfer upload datatype, on page 479
transfer upload mode, on page 482
transfer upload filename, on page 481
transfer upload path, on page 484
transfer upload serverip, on page 486
transfer upload start, on page 486

transfer download start

To initiate a download, use the **transfer download start** command.

transfer download start

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

The following example shows how to initiate a download:

```
(Cisco Controller) > transfer download start
Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... 172.16.16.78
TFTP Path................................ directory path
TFTP Filename............................ webadmincert_name
This may take some time.
Are you sure you want to start? (y/n) Y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

Related Topics

clear transfer, on page 38
transfer download mode, on page 472
transfer download certpasswor, on page 470
transfer download filename, on page 472
transfer download path, on page 474
transfer download serverip, on page 475
transfer download password, on page 473
transfer upload datatype, on page 479
transfer upload mode, on page 482
transfer upload filename, on page 481

transfer upload path, on page 484
transfer upload serverip, on page 486
transfer upload start, on page 486

transfer download tftpPktTimeout

To specify the TFTP packet timeout, use the **transfer download tftpPktTimeout** command.

transfer download tftpPktTimeout *timeout*

Syntax Description

timeout	Timeout in seconds between 1 and 254.

Command Default

None

Command History

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

The following example shows how to transfer a file with the TFTP packet timeout of 55 seconds:

```
(Cisco Controller) > transfer download tftpPktTimeout 55
```

Related Topics

clear transfer, on page 38
transfer download mode, on page 472
transfer download filename, on page 472
transfer download path, on page 474
transfer download serverip, on page 475
transfer download start, on page 476
transfer upload datatype, on page 479
transfer upload mode, on page 482
transfer upload filename, on page 481
transfer upload path, on page 484
transfer upload serverip, on page 486
transfer upload start, on page 486

transfer download tftpMaxRetries

To specify the number of allowed TFTP packet retries, use the **transfer download tftpMaxRetries** command.

transfer download tftpMaxRetries *retries*

Syntax Description

retries	Number of allowed TFTP packet retries between 1 and 254 seconds.

Command Default

None

Command History

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

The following example shows how to set the number of allowed TFTP packet retries to 55:

```
(Cisco Controller) > transfer download tftpMaxRetries 55
```

Related Topics

clear transfer, on page 38
transfer download mode, on page 472
transfer download filename, on page 472
transfer download path, on page 474
transfer download serverip, on page 475
transfer download start, on page 476
transfer upload datatype, on page 479
transfer upload mode, on page 482
transfer upload filename, on page 481
transfer upload path, on page 484
transfer upload serverip, on page 486
transfer upload start, on page 486

transfer download username

To specify the FTP username, use the **transfer download username** command.

transfer download username *username*

Syntax Description

username	Username.

Command Default

None

Command History

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

The following example shows how to set the FTP username to ftp_username:

```
(Cisco Controller) > transfer download username ftp_username
```

Related Topics

transfer download mode, on page 472
transfer download path, on page 474
transfer download password, on page 473

transfer encrypt

To configure encryption for configuration file transfers, use the **transfer encrypt** command.

transfer encrypt {**enable** | **disable** | **set-key** *key*}

Syntax Description

enable	Enables the encryption settings.
disable	Disables the encryption settings.
set-key	Specifies the encryption key for configuration file transfers.
key	Encryption key for config file transfers.

Command Default

None

Command History

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

The following example shows how to enable the encryption settings:

```
(Cisco Controller) > transfer encrypt enable
```

Related Topics

clear transfer, on page 38
transfer download mode, on page 472
transfer download filename, on page 472
transfer download path, on page 474
transfer download serverip, on page 475
transfer download start, on page 476
transfer upload datatype, on page 479
transfer upload mode, on page 482
transfer upload filename, on page 481
transfer upload path, on page 484
transfer upload serverip, on page 486
transfer upload start, on page 486

transfer upload datatype

To set the controller to upload specified log and crash files, use the **transfer upload datatype** command.

transfer upload datatype {**ap-crash-data** | **config** | **coredump** | **crashfile** | **debug-file** | **eapcacert** | **eapdevcert** | **errorlog** | **invalid-config** | **pac** | **packet-capture** | **panic-crash-file** | **radio-core-dump** | **rrm-log** | **run-config** | **signature** | **systemtrace** | **traplog** | **watchdog-crash-filewebadmincert** | **webauthbundle** | **webauthcert**}

Syntax Description

ap-crash-data	Uploads the AP crash files.
config	Uploads the system configuration file.
coredump	Uploads the core-dump file.
crashfile	Uploads the system crash file.
debug-file	Uploads the system's debug log file.
eapcacert	Uploads an EAP CA certificate.
eapdevcert	Uploads an EAP Dev certificate.
errorlog	Uploads the system error log file.
invalid-config	Uploads the system invalid-config file.
pac	Uploads a Protected Access Credential (PAC).
packet-capture	Uploads a packet capture file.
panic-crash-file	Uploads the kernel panic information file.
radio-core-dump	Uploads the system error log.
rrm-log	Uploads the system's trap log.
run-config	Upload the WLC's running configuration
signature	Uploads the system signature file.
systemtrace	Uploads the system trace file.
traplog	Uploads the system trap log.
watchdog-crash-file	Uploads a console dump file resulting from a software-watchdog-initiated controller reboot following a crash.
webadmincert	Uploads Web Admin certificate.
webauthbundle	Uploads a Web Auth bundle.
webauthcert	Upload a web certificate

Command Default

None

Command History

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

The following example shows how to upload the system error log file:

```
(Cisco Controller) > transfer upload datatype errorlog
```

Related Topics

clear transfer, on page 38
transfer upload filename, on page 481
transfer upload mode, on page 482
transfer upload pac, on page 482
transfer upload password, on page 483
transfer upload path, on page 484
transfer upload port, on page 485
transfer upload serverip, on page 486
transfer upload start, on page 486
transfer upload username, on page 487

transfer upload filename

To upload a specific file, use the **transfer upload filename** command.

transfer upload filename *filename*

Syntax Description

filename	Filename that contains up to 16 alphanumeric characters.

Command Default

None

Command History

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

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the filename.

The following example shows how to upload a file build603:

```
(Cisco Controller) > transfer upload filename build603
```

Related Topics

clear transfer, on page 38
transfer upload datatype, on page 479
transfer upload mode, on page 482
transfer upload pac, on page 482
transfer upload password, on page 483
transfer upload path, on page 484
transfer upload port, on page 485
transfer upload serverip, on page 486
transfer upload start, on page 486
transfer upload username, on page 487

transfer upload mode

To configure the transfer mode, use the **transfer upload mode** command.

transfer upload mode {**ftp** | **tftp** | **sftp**}

Syntax Description

ftp	Sets the transfer mode to FTP.
tftp	Sets the transfer mode to TFTP.
sftp	Sets the transfer mode to SFTP.

Command Default

None

Command History

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

The following example shows how to set the transfer mode to TFTP:

```
(Cisco Controller) > transfer upload mode tftp
```

Related Topics

clear transfer, on page 38
transfer upload datatype, on page 479
transfer upload filename, on page 481
transfer upload pac, on page 482
transfer upload password, on page 483
transfer upload path, on page 484
transfer upload port, on page 485
transfer upload serverip, on page 486
transfer upload start, on page 486
transfer upload username, on page 487

transfer upload pac

To load a Protected Access Credential (PAC) to support the local authentication feature and allow a client to import the PAC, use the **transfer upload pac** command.

transfer upload pac *username validity password*

Syntax Description

username	User identity of the PAC.
validity	Validity period (days) of the PAC.
password	Password to protect the PAC.

Command Default None

Command History

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

Usage Guidelines The client upload process uses a TFTP or FTP server.

The following example shows how to upload a PAC with the username user1, validity period 53, and password pass01:

```
(Cisco Controller) > transfer upload pac user1 53 pass01
```

Related Topics

clear transfer, on page 38
transfer upload datatype, on page 479
transfer upload filename, on page 481
transfer upload mode, on page 482
transfer upload password, on page 483
transfer upload path, on page 484
transfer upload port, on page 485
transfer upload serverip, on page 486
transfer upload start, on page 486
transfer upload username, on page 487

transfer upload password

To configure the password for FTP transfer, use the **transfer upload password** command.

Syntax Description

password	Password needed to access the FTP server.

transfer upload password *password*

Command Default None

Command History

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

The following example shows how to configure the password for the FTP transfer to pass01:

```
(Cisco Controller) > transfer upload password pass01
```

Related Topics

clear transfer, on page 38
transfer upload datatype, on page 479
transfer upload filename, on page 481

transfer upload mode, on page 482
transfer upload pac, on page 482
transfer upload port, on page 485
transfer upload path, on page 484
transfer upload serverip, on page 486
transfer upload start, on page 486
transfer upload username, on page 487

transfer upload path

To set a specific upload path, use the **transfer upload path** command.

transfer upload path *path*

Syntax Description		
	path	Server path to file.

Command Default None

Command History

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

Usage Guidelines You cannot use special characters such as \ : * ? " < > | for the file path.

The following example shows how to set the upload path to c:\install\version2:

```
(Cisco Controller) > transfer upload path c:\install\version2
```

Related Topics

clear transfer, on page 38
transfer upload datatype, on page 479
transfer upload filename, on page 481
transfer upload mode, on page 482
transfer upload pac, on page 482
transfer upload password, on page 483
transfer upload port, on page 485
transfer upload serverip, on page 486
transfer upload start, on page 486
transfer upload username, on page 487

transfer upload peer-start

To upload a file to the peer WLC, use the **transfer upload peer-start** command.

transfer upload peer-start

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

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

The following example shows how to start uploading a file to the peer controller:

```
(Cisco Controller) >transfer upload peer-start
Mode..................................... FTP
FTP Server IP.................................. 209.165.201.1
FTP Server Port................................ 21
FTP Path....................................... /builds/nimm/
FTP Filename................................... AS_5500_7_4_1_20.aes
FTP Username................................... wnbu
FTP Password................................... *********
Data Type...................................... Error Log

Are you sure you want to start upload from standby? (y/N) n

Transfer Canceled
```

transfer upload port

To specify the FTP port, use the **transfer upload port** command.

transfer upload port *port*

Syntax Description

port	Port number.

Command Default The default FTP port is 21.

Command History

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

The following example shows how to specify FTP port 23:

```
(Cisco Controller) > transfer upload port 23
```

Related Topics

clear transfer, on page 38
transfer upload datatype, on page 479
transfer upload filename, on page 481
transfer upload mode, on page 482
transfer upload pac, on page 482
transfer upload password, on page 483
transfer upload path, on page 484

transfer upload serverip, on page 486
transfer upload start, on page 486
transfer upload username, on page 487

transfer upload serverip

To configure the IPv4 or IPv6 address of the TFTP server to upload files to, use the **transfer upload serverip** command.

transfer upload serverip *IP addr*

Syntax Description

IP addr	TFTP Server IPv4 or IPv6 address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to set the IPv4 address of the TFTP server to 175.31.56.78:

```
(Cisco Controller) > transfer upload serverip 175.31.56.78
```

The following example shows how to set the IPv6 address of the TFTP server to 175.31.56.78:

```
(Cisco Controller) > transfer upload serverip 2001:10:1:1::1
```

Related Topics

clear transfer, on page 38
transfer upload datatype, on page 479
transfer upload filename, on page 481
transfer upload mode, on page 482
transfer upload pac, on page 482
transfer upload password, on page 483
transfer upload path, on page 484
transfer upload port, on page 485
transfer upload start, on page 486
transfer upload username, on page 487

transfer upload start

To initiate an upload, use the **transfer upload start** command.

transfer upload start

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

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

The following example shows how to initiate an upload of a file:

```
(Cisco Controller) > transfer upload start
Mode..................................... TFTP
TFTP Server IP........................... 172.16.16.78
TFTP Path................................ c:\find\off/
TFTP Filename............................ wps_2_0_75_0.aes
Data Type................................ Code
Are you sure you want to start? (y/n) n
Transfer Cancelled
```

Related Topics

clear transfer, on page 38
transfer upload datatype, on page 479
transfer upload filename, on page 481
transfer upload mode, on page 482
transfer upload pac, on page 482
transfer upload password, on page 483
transfer upload path, on page 484
transfer upload port, on page 485
transfer upload serverip, on page 486
transfer upload username, on page 487

transfer upload username

To specify the FTP username, use the **transfer upload username** command.

transfer upload username

Syntax Description

username	Username required to access the FTP server. The username can contain up to 31 characters.

Command Default None

Command History

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

The following example shows how to set the FTP username to ftp_username:

```
(Cisco Controller) > transfer upload username ftp_username
```

Related Topics

clear transfer, on page 38
transfer upload datatype, on page 479
transfer upload filename, on page 481
transfer upload mode, on page 482
transfer upload pac, on page 482
transfer upload password, on page 483
transfer upload path, on page 484
transfer upload port, on page 485
transfer upload serverip, on page 486
transfer upload start, on page 486

Installing and Modifying Licenses on Cisco 5500 Series Controllers

Use the **license** commands to install, remove, modify, or rehost licenses.

Note Some license commands are available only on the Cisco 5500 Series Controller. Right to Use (RTU) licensing is not supported on Cisco 5500 Series Controllers.

Note For detailed information on installing and rehosting licenses on the Cisco 5500 Series Controller, see the "Installing and Configuring Licenses" section in Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide*.

license clear

To remove a license from the Cisco 5500 Series Controller, use the **license clear** command.

license clear *license_name*

Syntax Description

license_name	Name of the license.

Command Default None

Command History

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

Usage Guidelines You can delete an expired evaluation license or any unused license. You cannot delete unexpired evaluation licenses, the permanent base image license, or licenses that are in use by the controller.

The following example shows how to remove the license settings of the license named wplus-ap-count:

```
(Cisco Controller) > license clear wplus-ap-count
```

Related Topics

license comment, on page 490
license install, on page 490
license revoke, on page 492
license save, on page 493
show license all, on page 404

license comment

To add comments to a license or delete comments from a license on the Cisco 5500 Series Controller, use the **license comment** command.

license comment {**add** | **delete**} *license_name comment_string*

Syntax Description

add	Adds a comment.
delete	Deletes a comment.
license_name	Name of the license.
comment_string	License comment.

Command Default None

Command History

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

The following example shows how to add a comment "wplus ap count license" to the license name wplus-ap-count:

```
(Cisco Controller) > license comment add wplus-ap-count Comment for wplus ap count license
```

Related Topics

license clear, on page 489
license install, on page 490
license revoke, on page 492
license save, on page 493
show license all, on page 404

license install

To install a license on the Cisco 5500 Series Controller, use the **license install** command.

license install *url*

Syntax Description

url	URL of the TFTP server (tftp://server_ip/path/filename).

Command Default None

Command History

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

Usage Guidelines

We recommend that the access point count be the same for the base-ap-count and wplus-ap-count licenses installed on your controller. If your controller has a base-ap-count license of 100 and you install a wplus-ap-count license of 12, the controller supports up to 100 access points when the base license is in use but only a maximum of 12 access points when the wplus license is in use.

You cannot install a wplus license that has an access point count greater than the controller's base license. For example, you cannot apply a wplus-ap-count 100 license to a controller with an existing base-ap-count 12 license. If you attempt to register for such a license, an error message appears indicating that the license registration has failed. Before upgrading to a wplus-ap-count 100 license, you would first have to upgrade the controller to a base-ap-count 100 or 250 license.

The following example shows how to install a license on the controller from the URL tftp://10.10.10.10/path/license.lic:

```
(Cisco Controller) > license install tftp://10.10.10.10/path/license.lic
```

Related Topics

license clear, on page 489
license revoke, on page 492
license save, on page 493
show license all, on page 404

license modify priority

To raise or lower the priority of the base-ap-count or wplus-ap-count evaluation license on a Cisco 5500 Series Controller, use the **license modify priority** command.

license modify priority *license_name* {**high** | **low**}

Syntax Description

license_name	Ap-count evaluation license.
high	Modifies the priority of an ap-count evaluation license.
low	Modifies the priority of an ap-count evaluation license.

Command Default

None

Command History

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

Usage Guidelines

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 50 access point count and want to try an evaluation license with a 100 access point count, you can try out the evaluation license for 60 days.

AP-count evaluation licenses are set to low priority by default so that the controller uses the ap-count permanent license. If you want to try an evaluation license with an increased access point count, you must change its priority to high. If you no longer want to have this higher capacity, you can lower the priority of the ap-count evaluation license, which forces the controller to use the permanent license.

Note You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.

Note If the ap-count evaluation license is a wplus license and the ap-count permanent license is a base license, you must also change the feature set to wplus.

Note To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

The following example shows how to set the priority of the wplus-ap-count to high:

```
(Cisco Controller) > license modify priority wplus-ap-count high
```

Related Topics

license install, on page 490
license clear, on page 489
license revoke, on page 492
license save, on page 493
show license all, on page 404

license revoke

To rehost a license on a Cisco 5500 Series WLC, use the **license revoke** command.

license revoke {*permission_ticket_url* | **rehost** *rehost_ticket_url*}

Syntax Description

permission_ticket_url	URL of the TFTP server (tftp://server_ip/path/filename) where you saved the permission ticket.
rehost	Specifies the rehost license settings.
rehost_ticket_url	URL of the TFTP server (tftp://server_ip/path/filename) where you saved the rehost ticket.

Command Default

None

Command History

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

Usage Guidelines

Before you revoke a license, save the device credentials by using the **license save credential** *url* command.

You can rehost all permanent licenses except the permanent base image license. Evaluation licenses and the permanent base image license cannot be rehosted.

In order to rehost a license, you must generate credential information from the controller and use it to obtain a permission ticket to revoke the license from the Cisco licensing site, https://tools.cisco.com/SWIFT/LicensingUI/Quickstart. Next, you must obtain a rehost ticket and use it to obtain a license installation file for the controller on which you want to install the license.

For detailed information on rehosting licenses, see the "Installing and Configuring Licenses" section in the *Cisco Wireless LAN Controller Configuration Guide*.

The following example shows how to revoke the license settings from the saved permission ticket URL tftp://10.10.10.10/path/permit_ticket.lic:

```
(Cisco Controller) > license revoke tftp://10.10.10.10/path/permit_ticket.lic
```

The following example shows how to revoke the license settings from the saved rehost ticket URL tftp://10.10.10.10/path/rehost_ticket.lic:

```
(Cisco Controller) > license revoke rehost tftp://10.10.10.10/path/rehost_ticket.lic
```

Related Topics

license install, on page 490
license clear, on page 489
license modify priority, on page 491
license save, on page 493
show license all, on page 404

license save

To save a backup copy of all installed licenses or license credentials on the Cisco 5500 Series Controller, use the **license save** command.

license save *credential url*

Syntax Description

credential	Device credential information.
url	URL of the TFTP server (tftp://server_ip/path/filename).

Command Default

None

Command History

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

Usage Guidelines

Save the device credentials before you revoke the license by using the **license revoke** command.

The following example shows how to save a backup copy of all installed licenses or license credentials on tftp://10.10.10.10/path/cred.lic:

```
(Cisco Controller) > license save credential tftp://10.10.10.10/path/cred.lic
```

Related Topics

license install, on page 490
license clear, on page 489
license modify priority, on page 491
license revoke, on page 492
show license all, on page 404

Troubleshooting the Controller Settings

debug arp

To configure the debugging of Address Resolution Protocol (ARP) options, use the **debug arp** command.

debug arp {**all** | **detail** | **events** | **message**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all ARP logs.
detail	Configures the debugging of ARP detail messages.
error	Configures the debugging of ARP errors.
message	Configures the debugging of ARP messages.
enable	Enables the ARP debugging.
disable	Disables the ARP debugging.

Command Default None

Command History

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

The following example shows how to enable ARP debug settings:

```
(Cisco Controller) > debug arp error enable
```

The following example shows how to disable ARP debug settings:

```
(Cisco Controller) > debug arp error disable
```

Related Commands

debug disable-all

show sysinfo

debug avc

To configure the debugging of Application Visibility and Control (AVC) options, use the **debug avc error** command.

debug avc {**events** | **error**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of AVC events.

error	Configures the debugging of AVC errors.
enable	Enables the debugging of AVC events or errors.
disable	Disables the debugging of AVC events or errors.

Command Default By default, the debugging of AVC options is disabled.

Command History

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

The following example shows how to enable the debugging of AVC errors:

```
(Cisco Controller) > debug avc error enable
```

Related Commands

config avc profile delete

config avc profile rule

config wlan avc

show avc profile

show avc applications

show avc statistics

debug cac

To configure the debugging of Call Admission Control (CAC) options, use the **debug cac** command.

debug cac {**all** | **event** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging options for all CAC messages.
event	Configures the debugging options for CAC events.
packet	Configures the debugging options for selected CAC packets.
kts	Configures the debugging options for KTS-based CAC messages.
enable	Enables the debugging of CAC settings.
disable	Disables the debugging of CAC settings.

Command Default By default, the debugging of CAC options is disabled.

Command History

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

The following example shows how to enable debugging of CAC settings:

```
(Cisco Controller) > debug cac event enable
(Cisco Controller) > debug cac packet enable
```

Related Commands

config 802.11 cac video acm

config 802.11 cac video max-bandwidth

config 802.11 video roam-bandwidth

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac voice load-based

config 802.11 cac voice roam-bandwidth

config 802.11cac voice stream-size

config 802.11cac voice tspec-inactivity-timeout

debug cdp

To configure debugging of CDP, use the **debug cdp** command.

debug cdp {**events** | **packets**} {**enable** | **disable**}

Syntax Description

events	Configures debugging of the CDP events.
packets	Configures debugging of the CDP packets.
enable	Enables debugging of the CDP options.
disable	Disables debugging of the CDP options.

Command Default

None

Command History

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

The following example shows how to enable CDP event debugging in a Cisco controller:

```
(Cisco Controller) > debug cdp
```

Related Topics

config cdp, on page 120

show cdp, on page 376

debug crypto

To configure the debugging of the hardware cryptographic options, use the **debug crypto** command.

debug crypto {**all** | **sessions** | **trace** | **warning**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all hardware crypto messages.
sessions	Configures the debugging of hardware crypto sessions.
trace	Configures the debugging of hardware crypto sessions.
warning	Configures the debugging of hardware crypto sessions.
enable	Enables the debugging of hardware cryptographic sessions.
disable	Disables the debugging of hardware cryptographic sessions.

Command Default

None

Command History

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

The following example shows how to enable the debugging of hardware crypto sessions:

```
(Cisco Controller) > debug crypto sessions enable
```

Related Commands

debug disable-all

show sysinfo

debug dhcp

To configure the debugging of DHCP, use the **debug dhcp** command.

debug dhcp {**message** | **packet**} {**enable** | **disable**}

Syntax Description

message	Configures the debugging of DHCP error messages.
packet	Configures the debugging of DHCP packets.
enable	Enables the debugging DHCP messages or packets.
disable	Disables the debugging of DHCP messages or packets.

Command Default None

The following example shows how to enable the debugging of DHCP messages:

```
(Cisco Controller) >debug dhcp message enable
```

debug dhcp service-port

To enable or disable debugging of the Dynamic Host Configuration Protocol (DHCP) packets on the service port, use the **debug dhcp service-port** command.

debug dhcp service-port {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of DHCP packets on the service port.
disable	Disables the debugging of DHCP packets on the service port.

Command Default None

Command History

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

The following example shows how to enable the debugging of DHCP packets on a service port:

```
(Cisco Controller) >debug dhcp service-port enable
```

debug disable-all

To disable all debug messages, use the **debug disable-all** command.

debug disable-all

Syntax Description This command has no arguments or keywords.

Command Default Disabled.

Command History

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

The following example shows how to disable all debug messages:

```
(Cisco Controller) > debug disable-all
```

debug fastpath

To debug the issues in the 10-Gigabit Ethernet interface of the controller and to view details of all the management and control features of the controller, use the **debug fastpath** command.

debug fastpath [{**disable** | **enable** | **errors** | **events** | **warning** | **log** | **status** | **dump** | **audit** | **clear**}]
debug fastpath log [{*error events show*}]
debug fastpath dump [{**stats** *DP_number*} | {**fpapool***DP_number*} | {**ownerdb**} | {**portdb**} | {**tun4db***indexDP_number*} | {**scbdb***indexDP_number*} | {**cfgtool -- dump.sfp**} | {**urlacldb***start-acl-id start-rule-index* } | {**vlandb**} | { **dpcp-stats**} | { **clear** *stats*} | {**systemdb**} | {**debug** | {**wlanappstats***wlan_id*}} | { **appqosdb**}]

Syntax Description

disable	Enables debug of fastpath messages.
enable	Disables debug of fastpath messages.
errors	Displays the debug messages related to the fastpath errors.
events	Displays the debug messages related to the fastpath events.
warnings	Displays the debug messages related to the fastpath warnings.
log	Configures debug of log messages.
errors	Configures debug of fastpath errors.
events	Configures debug of fastpath events.
show	Displays log of most recent events related to fastpath.
status	Displays status of fastpath configuration.
dump	Displays the CLI dump commands.
stats	Displays the debug statistics from the data plane.
DP_number	Displays the statistic counters at data plane based on selected data plane number. Values include 0, 1, and All. The default option is All. You must select: • The index 0 for the Cisco Wireless LAN Controller 2504 Series, Cisco Wireless LAN Controller 5508 Series, Cisco Wireless LAN Controller 7500 Series, Cisco Wireless LAN Controller 8500 Series. • The index 0 and/or 1 respectively for the two data planes in WiSM2 to view statistics of individual data plane or from both.
fpapool	Displays statistics of packet buffer in data plane.

DP_number	Displays statistics of packet buffer based on data plane number. Values include 0, 1, and All. The default option is All. You must select: • The index 0 for the Cisco Wireless LAN Controller 2504 Series, Cisco Wireless LAN Controller 5508 Series, Cisco Wireless LAN Controller 7500 Series, Cisco Wireless LAN Controller 8500 Series. • The index 0 and/or 1 respectively for the two data planes in WiSM2 to view statistics of individual data plane or from both.
ownerdb	Displays the data plane owner information.
portdb	Displays the port database at data plane.
tun4db	Dumps the first 20 tunnels from the data plane.
index	Dumps 20 tunnel entries from index provided. You must use data plane number 0/1 to denote WISM2 data plane processor.
DP_number	Dumps the first twenty client entries from the data plane. Values include 0, 1, and All. The default option is All. You must select: • The index 0 for the Cisco Wireless LAN Controller 2504 Series, Cisco Wireless LAN Controller 5508 Series, Cisco Wireless LAN Controller 7500 Series, Cisco Wireless LAN Controller 8500 Series. • The index 0 and/or 1 respectively for the two data planes in WiSM2 to view statistics of individual data plane or from both.
scbdb	Dumps 20 client entries starting from index provided. You must use data plane number 0/1 to denote WISM2 data plane processor.
index	Dumps client information for the selected MAC address.

DP_number	Dumps the first twenty client entries from the data plane. Values include 0, 1, and All. The default option is All. You must select: • The index 0 for the Cisco Wireless LAN Controller 2504 Series, Cisco Wireless LAN Controller 5508 Series, Cisco Wireless LAN Controller 7500 Series, Cisco Wireless LAN Controller 8500 Series. • The index 0 and/or 1 respectively for the two data planes in WiSM2 to view statistics of individual data plane or from both.
cfgtool -- dump.sfp	Displays the model/type of SX/LC/T small form-factor plug-in (SFP) modules with the OUI Partnumber.
urlacldb *start-acl-id start-rule-index*	Dumps the URL ACL database.
vlandb	Dumps the VLAN database in the dataplane.
dpcp-stats	Displays the dataplane to controlplane message statistics.
clear stats	Clears the data plane statistic counters.
systemdb	Displays the global data plane configuration.
debug	Displays the few latest messages of the data plane to enable troubleshooting.
wlanappstats	Displays Application Visibility and Control (AVC) statistics of a WLAN.
wlan_id	The WLAN identifier of the WLAN you need identify the AVC statistics.
appqosdb	Displays Application Visibility and Control (AVC) database statistics of the data plane.
clear	Clear command.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.3	This command was enhanced in this release. The new keyword added is urlacldb

Usage Guidelines

None

Examples

The following is an example of the SX/LC/T small form-factor plug-in (SFP) modules model/type with the respective OUI Partnumber.

```
(Cisco Controller) >debug fastpath status

           STP   Admin   Physical   Physical   Link   Link
Pr  Type   Stat   Mode     Mode      Status   Status  Trap     POE
SFPType
-- ------- ---- ------- ---------- ---------- ------ ------- -------
----------
1  Normal  Forw Enable  Auto       1000 Full  Up     Enable  N/A
1000BaseTX
2  Normal  Forw Enable  Auto       1000 Full  Up     Enable  N/A
1000BaseTX
```

The following is an example of the fastpath status displayed while you execute the status command.

```
 (Cisco Controller) >debug fastpath status

FP0.03:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.00:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.06:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.05:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.06:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.03:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.06:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.07:(119125)Received command: FP_CMD_ACL_COUNTER_GET
FP0.04:(119125)Received command: FP_CMD_ACL_COUNTER_GET
FP0.03:(119125)Received command: FP_CMD_ACL_COUNTER_GET
```

The following is an example of the fastpath errors displayed while you execute the debug fastpath log errors command.

```
(Cisco Controller) >debug fastpath log errors

FP0.04:(873365)[fp_ingress_capwap:429]Discarding Control/Data
Plane DTLS-Application packets after Lookup Failed
FP0.02:(873418)Change logDebugLevel from: 0x1e to 0x9
```

The following is an example of the fastpath events displayed while you execute the debug fastpath log events command.

```
(Cisco Controller) >debug fastpath log events

FP0.09:(873796)[fp_ingress_capwap:429]Discarding Control/Dat
a Plane DTLS-Application packets after Lookup Failed
FP0.06:(873921)Change logDebugLevel from: 0x9 to 0x1e
```

The following is an example displayed while you execute the debug fastpath log show command.

```
(Cisco Controller) >debug fastpath log show

FP0.07:(874033)Change logDebugLevel from: 0x1e to 0x9
Fastpath CPU0.02: FAST CACHE DISABLED
Fastpath CPU0.02: FAST CACHE ENABLED
Fastpath CPU0.00: Received command: FP_CMD_ADD_AP
Fastpath CPU0.05: Received command: FP_CMD_DEL_TUN4 ifTun=1113
```

```
Fastpath CPU0.03: Received command: FP_CMD_DEL_TUN4 ifTun=3161
Fastpath CPU0.03: Received command: FP_CMD_DEL_AP
FP0.02:[cmdDelMcastRgTun:6733]failed to delete mcast rg tun 0 ifTun=3161
FP0.07:[fp_ingress_capwap:429]Discarding Control/Data Plane
DTLS-Application packets after Lookup Failed
FP0.01:[fp_ingress_capwap:429]Discarding Control/Data Plane
DTLS-Application packets after Lookup Failed
Fastpath CPU0.01: Received command: FP_CMD_ADD_TUN4 type=CAPWAP ifTun=1114
 dstIP
=9.4.110.100 dstMac=2037.06e2.5ec4 dstIPv6=
0000:0000:0000:0000:0000:0000:0000:0000
Fastpath CPU0.01: Tunnel 1114 srcip=9041820 dstip=9046e64 xor=0x7644(30276)
 LAG Offset=0,0,0,0,1,0,1,4
Fastpath CPU0.09: Received command: FP_CMD_ADD_TUN4 type=CAPWAP ifTun=3162
 dstIP
=9.4.110.100 dstMac=2037.06e2.5ec4 dstIPv6=
0000:0000:0000:0000:0000:0000:0000:0000
Fastpath CPU0.09: Tunnel 3162 srcip=9041820 dstip=9046e64 xor=0x7644(30276)
 LAG Offset=0,0,0,0,1,0,1,4
Fastpath CPU0.00: Received command: FP_CMD_SET_INTERFACE_MTU
Fastpath CPU0.00: FAST CACHE DISABLED
Fastpath CPU0.00: FAST CACHE ENABLED
Fastpath CPU0.00: Received command: FP_CMD_ADD_AP
Fastpath CPU0.03: Received command: FP_CMD_UPDATE_EOIP for index=5122
Fastpath CPU0.02: Received command: FP_CMD_UPDATE_EOIP for index=5122
Fastpath CPU0.00: Received command: FP_CMD_DEL_TUN4 ifTun=1114
Fastpath CPU0.03: Received command: FP_CMD_DEL_TUN4 ifTun=3162
Fastpath CPU0.03: Received command: FP_CMD_DEL_AP
FP0.04:[cmdDelMcastRgTun:6733]failed to delete mcast rg tun 0 ifTun=3162
```

debug flexconnect avc

To debug a Flexconnect Application Visibility and Control (AVC) event, use the **debug flexconnect avc** command.

debug flexconnect ave {**event** | **error** | **detail**} {**enable** | **disable**}

Syntax Description

event	Debugsa FlexConnect AVC event.
error	Debugs a FlexConnect AVC error.
detail	Debugs a FlexConnect AVC details.
enable	Enables debug.
disable	Disables debug.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable a debug action for an event:

```
(Cisco Controller) >debug flexconnect avc event enable
```

debug l2age

To configure the debugging of Layer 2 age timeout messages, use the **debug l2age** command.

debug l2age {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of Layer2 age settings.
disable	Disables the debugging Layer2 age settings.

Command Default None

Command History

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

The following example shows how to enable the debugging of Layer2 age settings:

```
(Cisco Controller) > debug l2age enable
```

Related Commands **debug disable-all**

debug mac

To configure the debugging of the client MAC address, use the **debug mac** command.

debug mac {**disable** | **addr** *MAC*}

Syntax Description

disable	Disables the debugging of the client using the MAC address.
addr	Configures the debugging of the client using the MAC address.
MAC	MAC address of the client.

Command Default None

Command History

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

The following example shows how to configure the debugging of the client using the MAC address:

```
(Cisco Controller) > debug mac addr 00.0c.41.07.33.a6
```

Related Commands **debug disable-all**

debug mdns all

To debug all multicast DNS (mDNS) messages, details, and errors, use the **debug mdns all** command.

debug mdns all {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of all mDNS messages, details, and errors.
disable	Disables the debugging of all mDNS messages, details, and errors.

Command Default By default, the debugging of all mDNS messages, details, and errors is disabled.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to enable debugging of all mDNS messages, details, and errors:

```
(Cisco Controller) > debug mdns all enable
```

Related Commands

config mdns profile

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns error

debug mdns detail

debug mdns detail

To debug multicast DNS (mDNS) details, use the **debug mdns detail** command.

debug mdns detail {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of mDNS details.
disable	Disables the debugging of mDNS details.

Command Default

This command is disabled by default.

Command History

Release	Modification
7.4	This command was introduced.

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

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

Related Commands

config mdns profile
config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns all
debug mdns error

debug mdns error

To debug multicast DNS (mDNS) errors, use the **debug mdns error** command.

debug mdns error {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of mDNS errors.
disable	Disables the debugging of mDNS errors.

Command Default This command is disabled by default.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to enable the debugging of mDNS errors.

```
(Cisco Controller) > debug mdns error enable
```

Related Commands

config mdns profile
config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns all
debug mdns detail
debug mdns message

debug mdns message

To debug multicast DNS (mDNS) messages, use the **debug mdns message** command.

debug mdns message {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of mDNS messages.
disable	Disables the debugging of mDNS messages.

Command Default Disabled.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to enable the debugging of mDNS messages:

```
(Cisco Controller) > debug mdns message enable
```

Related Commands

config mdns profile

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug memory

To enable or disable the debugging of errors or events during the memory allocation of the Cisco WLC, use the **debug memory** command.

debug memory {**errors** | **events**} {**enable** | **disable**}

Syntax Description

errors	Configures the debugging of memory leak errors.
events	Configures debugging of memory leak events.
enable	Enables the debugging of memory leak events.
disable	Disables the debugging of memory leak events.

Command Default

By default, the debugging of errors or events during the memory allocation of the Cisco WLC is disabled.

Command History

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

The following example shows how to enable the debugging of memory leak events:

```
(Cisco Controller) > debug memory events enable
```

Related Commands

config memory monitor errors

show memory monitor

config memory monitor leaks

debug nmsp

To configure the debugging of the Network Mobility Services Protocol (NMSP), use the **debug nmsp** command.

debug nmsp {**all** | **connection** | **detail** | **error** | **event** | **message** | **packet**}

Syntax Description

all	Configures the debugging for all NMSP messages.
connection	Configures the debugging for NMSP connection events.
detail	Configures the debugging for NMSP events in detail.
error	Configures the debugging for NMSP error messages.
event	Configures the debugging for NMSP events.
message	Configures the debugging for NMSP transmit and receive messages.
packet	Configures the debugging for NMSP packet events.

Command Default

None

Command History

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

The following example shows how to configure the debugging of NMSP connection events:

```
(Cisco Controller) > debug nmsp connection
```

Related Commands

clear nmsp statistics

debug disable-all

config nmsp notify-interval measurement

debug ntp

To configure the debugging of the Network Time Protocol (NTP), use the **debug ntp** command.

debug ntp {**detail** | **low** | **packet**} {**enable** | **disable**}

Syntax Description

detail	Configures the debugging of detailed NTP messages.
low	Configures the debugging of NTP messages.

packet	Configures the debugging of NTP packets.
enable	Enables the NTP debugging.
disable	Disables the NTP debugging.

Command Default None

Command History

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

The following example shows how to enable the debugging of NTP settings:

```
(Cisco Controller) > debug ntp packet enable
```

Related Commands **debug disable-all**

debug packet error

To configure debugging of the packets sent to the Cisco Wireless LAN Controller (WLC) CPU , use the **debug packet error** command.

debug packet error {**enable** | **disable**}

Syntax Description

enable	Enables debugging of the packets sent to the Cisco WLC CPU.
disable	Disables debugging of the packets sent to the Cisco WLC CPU.

Command Default None

Command History

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

The following example shows how to enable the debugging of the packets sent to the Cisco WLC CPU:

```
(Cisco Controller) > debug packet error enable
```

Related Topics

debug packet logging, on page 511

debug packet logging

To configure logging of the packets sent to the Cisco Wireless LAN Controller CPU, use the **debug packet logging** command.

debug packet logging {**acl** | **disable** | **enable** {**rx** | **tx** | **all**} *packet_count display_size* | **format** {**hex2pcap** | **text2pcap**}}

debug packet logging acl {**clear-all** | **driver** *rule_index action npu_encap port* | **eoip-eth** *rule_index action dst src type vlan* | **eoip-ip** *rule_index action src dst proto src_port dst_port* | **eth** *rule_index action dst src type vlan* | **ip** *rule_index action src dst proto src_port dst_port* | **lwapp-dot11***rule_index action dst src bssid type* | **lwapp-ip** *rule_index action src dst proto src_port dst_port*}

Syntax Description

acl	Filters the displayed packets according to a rule.
disable	Disables logging of all the packets.
enable	Enables logging of all the packets.
rx	Displays all the received packets.
tx	Displays all the transmitted packets.
all	Displays both the transmitted and the received packets.
packet_count	Maximum number of packets to be logged. The range is from 1 to 65535. The default value is 25.
display_size	Number of bytes to be displayed when printing a packet. By default, the entire packet is displayed.
format	Configures the format of the debug output.
hex2pcap	Configures the output format to be compatible with the hex2pcap format. The standard format used by Cisco IOS supports the use of hex2pcap and can be decoded using an HTML front end.
text2pcap	Configures the output format to be compatible with the text2pcap format. In this format, the sequence of packets can be decoded from the same console log file. .
clear-all	Clears all the existing rules pertaining to the packets.
driver	Filters the packets based on an incoming port or a Network Processing Unit (NPU) encapsulation type.
rule_index	Index of the rule that is a value between 1 and 6 (inclusive).
action	Action for the rule, which can be **permit**, **deny**, or **disable**.
npu_encap	NPU encapsulation type that determines how the packets are filtered. The possible values are *dhcp, dot11-mgmt, dot11-probe, dot1x, eoip-ping, iapp, ip, lwapp, multicast, orphan-from-sta, orphan-to-sta, rbcp, wired-guest,* or *any*.
port	Physical port for packet transmission or reception.
eoip-eth	Filters packets based on the Ethernet II header in the Ethernet over IP (EoIP) payload.

dst	Destination MAC address.
src	Source MAC address.
type	Two-byte type code, such as 0x800 for IP, 0x806 for Address Resolution Protocol (ARP). You can also enter a few common string values such as *ip* (for 0x800) or *arp* (for 0x806).
vlan	Two-byte VLAN identifier.
eoip-ip	Filters packets based on the IP header in the EoIP payload.
proto	Protocol. Valide values are: *ip, icmp, igmp, ggp, ipencap, st, tcp, egp, pup, udp, hmp, xns-idp, rdp, iso-tp4, xtp, ddp, idpr-cmtp, rspf, vmtp, ospf, ipip,* and *encap*.
src_port	User Datagram Protocol or Transmission Control Protocol (UDP or TCP) two-byte source port, such as *telnet, 23* , or *any*. The Cisco WLC supports the following strings: *tcpmux, echo, discard, systat, daytime, netstat, qotd, msp, chargen, ftp-data, ftp, fsp, ssh, telnet, smtp, time, rlp, nameserver, whois, re-mail-ck, domain, mtp, bootps, bootpc, tftp, gopher, rje, finger, www, link, kerberos, supdup, hostnames, iso-tsap, csnet-ns, 3com-tsmux, rtelnet, pop-2, pop-3, sunrpc, auth, sftp, uucp-path, nntp, ntp, netbios-ns, netbios-dgm, netbios-ssn, imap2, snmp, snmp-trap, cmip-man, cmip-agent, xdmcp, nextstep, bgp, prospero, irc, smux, at-rtmp, at-nbp, at-echo, at-zis, qmtp, z3950, ipx, imap3, ulistserv, https, snpp, saft, npmp-local, npmp-gui,* and *hmmp-ind*.
dst_port	UDP or TCP two-byte destination port, such as *telnet, 23*, or *any*. The Cisco WLC supports the same strings as those for the src_port.
eth	Filters packets based on the values in the Ethernet II header.
ip	Filters packets based on the values in the IP header.
lwapp-dot11	Filters packets based on the 802.11 header in the Lightweight Access Point Protocol (LWAPP) payload.
bssid	Basic Service Set Identifier of the VLAN.
lwapp-ip	Filters packets based on the IP header in the LWAPP payload.

Command Default

None

Command History

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

The following example shows how to enable logging of a packet:

```
(Cisco Controller) > debug packet logging enable
```

Related Topics

debug packet error, on page 511

debug poe

To configure the debugging of Power over Ethernet (PoE), use the **debug poe** command.

debug poe {**detail** | **message** | **error**} {**enable** | **disable**}

Syntax Description

detail	Configures the debugging of PoE detail logs.
error	Configures the debugging of PoE error logs.
message	Configures the debugging of PoE messages.
enable	Enables the debugging of PoE logs.
disable	Disables the debugging of PoE logs.

Command Default

None

Command History

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

The following example shows how to enable the PoE debugging:

```
(Cisco Controller) > debug poe message enable
```

Related Commands

debug disable-all

debug rbcp

To configure Router Blade Control (RBCP) debug options, use the **debug rbcp** command.

debug rbcp {**all** | **detail** | **errors** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of RBCP.
detail	Configures the debugging of RBCP detail.
errors	Configures the debugging of RBCP errors.
packet	Configures the debugging of RBCP packet trace.
enable	Enables the RBCP debugging.
disable	Disables the RBCP debugging.

Command Default None

The following example shows how to enable the debugging of RBCP settings:

```
(Cisco Controller) > debug rbcp packet enable
```

Related Commands **debug disable-all**

debug rfid

To configure radio frequency identification (RFID) debug options, use the **debug rfid** command.

debug rfid {**all** | **detail** | **errors** | **nmsp** | **receive**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all RFID.
detail	Configures the debugging of RFID detail.
errors	Configures the debugging of RFID error messages.
nmsp	Configures the debugging of RFID Network Mobility Services Protocol (NMSP) messages.
receive	Configures the debugging of incoming RFID tag messages.
enable	Enables the RFID debugging.
disable	Disables the RFID debugging.

Command Default None

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

```
(Cisco Controller) > debug rfid errors enable
```

Related Commands **debug disable-all**

debug snmp

To configure SNMP debug options, use the **debug snmp** command.

debug snmp {**agent** | **all** | **mib** | **trap**} {**enable** | **disable**}

Syntax Description

agent	Configures the debugging of the SNMP agent.
all	Configures the debugging of all SNMP messages.
mib	Configures the debugging of the SNMP MIB.

trap	Configures the debugging of SNMP traps.
enable	Enables the SNMP debugging.
disable	Disables the SNMP debugging.

Command Default None

The following example shows how to enable the SNMP debugging:

```
(Cisco Controller) > debug snmp trap enable
```

Related Commands **debug disable-all**

debug transfer

To configure transfer debug options, use the **debug transfer** command.

debug transfer {**all** | **tftp** | **trace**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all transfer messages.
tftp	Configures the debugging of TFTP transfers.
trace	Configures the debugging of transfer messages.
enable	Enables the debugging of transfer messages.
disable	Disables the debugging of transfer messages.

Command Default None

The following example shows how to enable the debugging of transfer messages:

```
(Cisco Controller) > debug transfer trace enable
```

Related Commands **debug disable-all**

debug voice-diag

To trace call or packet flow, use the **debug voice-diag** command.

debug voice-diag {**enable** *client_mac1* [*client_mac2*] [**verbose**] | **disable**}

Syntax Description

enable	Enables the debugging of voice diagnostics for voice clients involved in a call.
client_mac1	MAC address of a voice client.

client_mac2	(Optional) MAC address of an additional voice client. **Note** Voice diagnostics can be enabled or disabled for a maximum of two voice clients at a time.
verbose	(Optional) Enables debug information to be displayed on the console. **Note** When voice diagnostics is enabled from the NCS or Prime Infrastructure, the verbose option is not available.
disable	Disables the debugging of voice diagnostics for voice clients involved in a call.

Command Default None

Usage Guidelines Follow these guidelines when you use the **debug voice-diag** command:

- When the command is entered, the validity of the clients is not checked.
- A few output messages of the command are sent to the NCS or Prime Infrastructure.
- The command expires automatically after 60 minutes.
- The command provides the details of the call flow between a pair of client MACs involved in an active call.

Note Voice diagnostics can be enabled for a maximum of two voice clients at a time.

The following example shows how to enable transfer/upgrade settings:

```
(Cisco Controller) > debug voice-diag enable 00:1a:a1:92:b9:5c 00:1a:a1:92:b5:9c verbose
```

Related Commands **show client voice-diag**

show client calls

show debug

To determine if the MAC address and other flag debugging is enabled or disabled, sse the **show debug** command.

show debug [**packet**]

Syntax Description

packet	Displays information about packet debugs.

Command Default

None.

This example shows how to display if debugging is enabled:

```
> show debug
MAC debugging.............................. disabled
Debug Flags Enabled:
  arp error enabled.
  bcast error enabled.
```

This example shows how to display if debugging is enabled:

```
> show debug packet
Status..................................... disabled
Number of packets to display..................... 0
Bytes/packet to display.......................... 0
Packet display format............................ text2pcap
   Driver ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-Dot11 ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-IP ACL:
      [1]: disabled
      [2]: disabled
```

```
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
```

Related Commands **debug mac**

show eventlog

To display the event log, use the **show eventlog** command.

show eventlog

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

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

The following is a sample output of the **show eventlog** command:

```
(Cisco Controller) > show eventlog
                                                    Time
       File     Line TaskID   Code        d  h  m  s
EVENT> bootos.c  788 125CEBCC AAAAAAAA    0  0  0  6
EVENT> bootos.c  788 125CEBCC AAAAAAAA    0  0  0  6
EVENT> bootos.c  788 125C597C AAAAAAAA    0  0  0  6
EVENT> bootos.c  788 125C597C AAAAAAAA    0  0  0  6
EVENT> bootos.c  788 125C597C AAAAAAAA    0  0  0  6
EVENT> bootos.c  788 125C597C AAAAAAAA    0  0  0  6
EVENT> bootos.c  788 125C597C AAAAAAAA    0  0  0  6
EVENT> bootos.c  788 125C597C AAAAAAAA    0  0  0  6
EVENT> bootos.c  788 1216C36C AAAAAAAA    0  0  0  6
EVENT> bootos.c  788 1216C36C AAAAAAAA    0  0  0  6
EVENT> bootos.c  788 1216C36C AAAAAAAA    0  0  0 11
```

show memory

To see system memory details, use the **show memory** command:

show memory {**history** | **pools summary** | **statistics** | **summary**}

Syntax Description

history	Displays system memory usage history statistics
pools summary	Queries Memory pool per task allocations
statistics	Displays system memory usage statistics
summary	Displays summary of system memory usage statistics

Command History

Release	Modification
7.6	This command was introduced in a release that is earlier than Release 7.6.
8.1	The **history, pools summary, and summary** parameters were introduced.

This example shows a sample output of**show memory summary** command:

```
(Cisco Controller) >show memory summary

------------------------- System Memory Summary -------------------------
System Name:WLC-5500 Primary SW Ver:8.x.x.x
Current Time:xxx System UP Time:1 days 21 hrs 37 mins 22 secs
NAME: "xxxxx"    , DESCR: "Cisco 5500 Series Wireless LAN Controller"
PID: AIR-CT5508-K9,  VID: V01,  SN: xxxxxxxxxxx
Total System Memory.............................. (1003656    KB) 980 MB
Total System Free Memory......................... (357592     KB) 349 MB (35 %)
Total Memory in Buffers.......................... (964        KB)
Total Memory in Cache............................ (164132     KB) 160 MB
Total Active Memory.............................. (524136     KB) 511 MB
Total InActive Memory............................ (61232      KB) 59 MB
Total Memory in Anon Pages....................... (420272     KB) 410 MB
Total Memory in Slab............................. (45988      KB) 44 MB
Total Memory in Page Tables...................... (1988       KB) 1 MB
WLC Peak Memory.................................. (954964     KB) 932 MB
WLC Virtual Memory Size.......................... (883460     KB) 862 MB
WLC Resident Memory.............................. (445392     KB) 434 MB
WLC Data Segment Memory.......................... (810332     KB) 791 MB
Total Heap Including Mapped Pages................ (338440     KB) 330 MB
Total Memory in Pmalloc Pools.................... (337183     KB) 329 MB
Total Used Memory in Pmalloc Pools............... (324561     KB) 316 MB
Total Free Memory in Pmalloc Pools............... (9238       KB) 9 MB

--More-- or (q)uit
------------------------ Pmalloc Pools Information --------------------
Index Pool-Size Chunks-In-Pool Chunks-In-Use Memory(Size/Used/Free)KB
0     16        50000          12347         3320    /2731    /588
1     64        40000          30787         4531    /3955    /575
2     128       20000          12457         3515    /2572    /942
3     256       3000           601           902     /302     /599
4     384       6000           92            2554    /339     /2215
5     512       18000          17953         9914    /9890    /23
6     1024      3500           106           3677    /283     /3394
7     2048      1000           727           2050    /1504    /546
8     4096      1425           1336          5772    /5416    /356
9     Raw-Pool  0              306           300932  /300932  /0
------------------------  MBUF Information ----------------------------
Maximum number of Mbufs.......................... 4608
Number of Mbufs Free............................. 4592
Number of Mbufs In Use........................... 16
```

This example shows a sample output of**show memory statistics** command:

```
(Cisco Controller) >show memory statistics

System Memory Statistics:
```

```
Total System Memory.............: 1027743744 bytes (980.20 MB)
Used System Memory..............: 487723008 bytes (465.16 MB)
Free System Memory..............: 540020736 bytes (515.04 MB)
Bytes allocated from RTOS......: 27239228 bytes (25.97 MB)
Chunks Free.....................: 8 bytes
Number of mmapped regions......: 51
Total space in mmapped regions.: 319324160 bytes (304.55 MB)
Total allocated space..........: 26654548 bytes (25.42 MB)
Total non-inuse space..........: 584680 bytes (570.97 KB)
Top-most releasable space......: 436888 bytes (426.64 KB)
Total allocated (incl mmap).....: 346563388 bytes (330.53 MB)
Total used (incl mmap).........: 345978708 bytes (329.97 MB)
Total free (incl mmap).........: 584680 bytes (570.97 KB)
```

show memory monitor

To display a summary of memory analysis settings and any discovered memory issues, use the **show memory monitor** command.

show memory monitor [**detail**]

Syntax Description

detail	(Optional) Displays details of any memory leaks or corruption.

Command Default

None

Command History

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

Usage Guidelines

Be careful when changing the defaults for the **config memory monitor** command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

The following is a sample output of the **show buffers** command:

```
(Cisco Controller) > show memory monitor
Memory Leak Monitor Status:
low_threshold(10000), high_threshold(30000), current status(disabled)
-----------------------------------------
Memory Error Monitor Status:
Crash-on-error flag currently set to (disabled)
No memory error detected.
```

The following is a sample output of the **show memory monitor detail** command:

```
(Cisco Controller) > show memory monitor detail
Memory error detected. Details:
-----------------------------------------------
- Corruption detected at pmalloc entry address:        (0x179a7ec0)
- Corrupt entry:headerMagic(0xdeadf00d),trailer(0xabcd),poison(0xreadceef),
entrysize(128),bytes(100),thread(Unknown task name,task id = (332096592)),
file(pmalloc.c),line(1736),time(1027)
Previous 1K memory dump from error location.
-----------------------------------------------
```

```
(179a7ac0): 00000000 00000000 00000000 ceeff00d readf00d 00000080 00000000 00000000
(179a7ae0): 17958b20 00000000 1175608c 00000078 00000000 readceef 179a7afc 00000001
(179a7b00): 00000003 00000006 00000001 00000004 00000001 00000009 00000009 0000020d
(179a7b20): 00000001 00000002 00000002 00000001 00000004 00000000 00000000 5d7b9aba
(179a7b40): cbddf004 192f465e 7791acc8 e5032242 5365788c a1b7cee6 00000000 00000000
(179a7b60): 00000000 00000000 00000000 00000000 00000000 ceeff00d readf00d 00000080
(179a7b80): 00000000 00000000 17958dc0 00000000 1175608c 00000078 00000000 readceef
(179a7ba0): 179a7ba4 00000001 00000003 00000006 00000001 00000004 00000001 00003763
(179a7c00): 1722246c 1722246c 00000000 00000000 00000000 00000000 00000000 ceeff00d
(179a7c20): readf00d 00000080 00000000 00000000 179a7b78 00000000 1175608c 00000078
...
```

Related Topics

config memory monitor errors, on page 189
config memory monitor leaks, on page 190
debug memory, on page 509

show run-config

To display a comprehensive view of the current Cisco wireless LAN controller configuration, use the command.

Syntax Description

all	Shows all the commands under the show run-config.
no-ap	(Optional) Excludes access point configuration settings.
commands	(Optional) Displays a list of user-configured commands on the controller.

Command Default

None

Command History

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

Usage Guidelines

These commands have replaced the **show running-config** command.

Some WLAN controllers may have no Crypto Accelerator (VPN termination module) or power supplies listed because they have no provisions for VPN termination modules or power supplies.

The **show run-config all** command shows only values configured by the user. It does not show system-configured default values.

The following is a sample output of the command:

```
(Cisco Controller) > show run-config all
Press Enter to continue...
System Inventory
Switch Description.............................. Cisco Controller
Machine Model...................................
Serial Number.................................. FLS0923003B
Burned-in MAC Address.......................... xx:xx:xx:xx:xx:xx
```

```
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK
Press Enter to continue Or <Ctl Z> to abort...
```

show process

To display how various processes in the system are using the CPU at that instant in time, use the **show process** command.

show process {**cpu** | **memory**}

Syntax Description

cpu	Displays how various system tasks are using the CPU at that moment.
memory	Displays the allocation and deallocation of memory from various processes in the system at that moment.

Command Default

None.

Usage Guidelines

This command is helpful in understanding if any single task is monopolizing the CPU and preventing other tasks from being performed.

This example shows how to display various tasks in the system that are using the CPU at a given moment:

```
> show process cpu
Name    Priority    CPU Use    Reaper
 reaperWatcher    ( 3/124)    0 %   ( 0/ 0)%    I
 osapiReaper    (10/121)    0 %    ( 0/ 0)%    I
 TempStatus    (255/ 1)    0 %    ( 0/ 0)%    I
 emWeb    (255/ 1)    0 %    ( 0/ 0)%    T 300
 cliWebTask    (255/ 1)    0 %    ( 0/ 0)%    I
 UtilTask    (255/ 1)    0 %    ( 0/ 0)%    T 300
```

This example shows how to display the allocation and deallocation of memory from various processes at a given moment:

```
> show process memory
Name    Priority    BytesinUse    Reaper
 reaperWatcher    ( 3/124)    0   ( 0/ 0)%    I
 osapiReaper    (10/121)    0    ( 0/ 0)%    I
 TempStatus    (255/ 1)    308    ( 0/ 0)%    I
 emWeb    (255/ 1)    294440    ( 0/ 0)%    T 300
 cliWebTask    (255/ 1)    738    ( 0/ 0)%    I
 UtilTask    (255/ 1)    308    ( 0/ 0)%    T 300
```

Related Commands

debug memory

transfer upload datatype

show tech-support

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support** command.

show tech-support

Syntax Description This command has no arguments or keywords.

Command Default None.

This example shows how to display system resource information:

```
> show tech-support
Current CPU Load..............................  0%
System Buffers
   Max Free Buffers...........................  4608
   Free Buffers...............................  4604
   Buffers In Use.............................  4
Web Server Resources
   Descriptors Allocated......................  152
   Descriptors Used...........................  3
   Segments Allocated.........................  152
   Segments Used..............................  3
System Resources
   Uptime.....................................  747040 Secs
   Total Ram..................................  127552 Kbytes
   Free Ram...................................  19540 Kbytes
   Shared Ram.................................  0 Kbytes
   Buffer Ram.................................  460 Kbytes
```

config memory monitor errors

To enable or disable monitoring for memory errors and leaks, use the **config memory monitor errors** command.

config memory monitor errors {**enable** | **disable**}

Caution The **config memory monitor** commands can be disruptive to your system and should be run only when you are advised to do so by the Cisco TAC.

Syntax Description

enable	Enables the monitoring for memory settings.
disable	Disables the monitoring for memory settings.

Command Default Monitoring for memory errors and leaks is disabled by default.

Command History

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

Usage Guidelines

Be cautious about changing the defaults for the **config memory monitor** command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

The following example shows how to enable monitoring for memory errors and leaks for a controller:

```
(Cisco Controller) > config memory monitor errors enable
```

Related Commands

config memory monitor leaks

debug memory

show memory monitor

config memory monitor leaks

To configure the controller to perform an auto-leak analysis between two memory thresholds, use the **config memory monitor leaks** command.

config memory monitor leaks *low_thresh high_thresh*

Caution The **config memory monitor** commands can be disruptive to your system and should be run only when you are advised to do so by the Cisco TAC.

Syntax Description

low_thresh	Value below which free memory cannot fall without crashing. This value cannot be set lower than 10000 KB.
high_thresh	Value below which the controller enters auto-leak-analysis mode. See the "Usage Guidelines" section.

Command Default

The default value for *low_thresh* is 10000 KB; the default value for *high_thresh* is 30000 KB.

Command History

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

Usage Guidelines

Note Be cautious about changing the defaults for the **config memory monitor** command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

Use this command if you suspect that a memory leak has occurred.

If the free memory is lower than the *low_thresh* threshold, the system crashes, generating a crash file. The default value for this parameter is 10000 KB, and you cannot set it below this value.

Set the *high_thresh* threshold to the current free memory level or higher so that the system enters auto-leak-analysis mode. After the free memory reaches a level lower than the specified *high_thresh* threshold, the process of tracking and freeing memory allocation begins. As a result, the **debug memory events enable** command shows all allocations and frees, and the **show memory monitor detail** command starts to detect any suspected memory leaks.

The following example shows how to set the threshold values for auto-leak-analysis mode to 12000 KB for the low threshold and 35000 KB for the high threshold:

```
(Cisco Controller) > config memory monitor leaks 12000 35000
```

Related Commands

config memory monitor leaks

debug memory

show memory monitor

config msglog level critical

To reset the message log so that it collects and displays only critical (highest-level) messages, use the **config msglog level critical** command.

config msglog level critical

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

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

Usage Guidelines The message log always collects and displays critical messages, regardless of the message log level setting.

The following example shows how to configure the message log severity level and display critical messages:

```
(Cisco Controller) > config msglog level critical
```

Related Commands

show msglog

config msglog level error

To reset the message log so that it collects and displays both critical (highest-level) and error (second-highest) messages, use the **config msglog level error** command.

config msglog level error

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

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

The following example shows how to reset the message log to collect and display critical and noncritical error messages:

```
(Cisco Controller) > config msglog level error
```

Related Commands **show msglog**

config msglog level security

To reset the message log so that it collects and displays critical (highest-level), error (second-highest), and security (third-highest) messages, use the **config msglog level security** command.

config msglog level security

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

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

The following example shows how to reset the message log so that it collects and display critical, noncritical, and authentication or security-related errors:

```
(Cisco Controller) > config msglog level security
```

Related Commands **show msglog**

config msglog level verbose

To reset the message log so that it collects and displays all messages, use the **config msglog level verbose** command.

config msglog level verbose

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

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

The following example shows how to reset the message logs so that it collects and display all messages:

```
(Cisco Controller) > config msglog level verbose
```

Related Commands **show msglog**

config msglog level warning

To reset the message log so that it collects and displays critical (highest-level), error (second-highest), security (third-highest), and warning (fourth-highest) messages, use the **config msglog level warning** command.

config msglog level warning

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

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

The following example shows how to reset the message log so that it collects and displays warning messages in addition to critical, noncritical, and authentication or security-related errors:

```
(Cisco Controller) > config msglog level warning
```

Related Commands **show msglog**

ping

To send ICMP echo packets to a specified IP address, use the ping command:

ping *ip-addr interface-name*

Syntax Description

ip-addr	IP address of the interface that you are trying to send ICMP echo packets to
interface-name	Name of the interface to which you are trying to send ICMP echo packets

Command Default None

Command History

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

Usage Guidelines

When you run the **ping** command, the CPU spikes up to 98 percent in the “osapi_ping_rx process”. While the **ping** command is running, the terminal and web activity on the Cisco WLC is blocked.

Example

The following example shows how to send ICMP echo packets to an interface:

```
(Cisco Controller) >ping 209.165.200.225 dyn-interface-1
```