System Management Commands

show Commands

This section lists the **show** commands that you can use to display information about the controller settings and user accounts.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 boot

To display the primary and backup software build numbers with an indication of which is active, use the **show boot** command.

show boot

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines Each Cisco wireless LAN controller retains one primary and one backup operating system software load in nonvolatile RAM to allow controllers to boot off the primary load (default) or revert to the backup load when desired.

The following is a sample output of the **show boot** command:

```
(Cisco Controller) > show boot
Primary Boot Image.............................. 3.2.13.0 (active)
Backup Boot Image............................... 3.2.15.0
```

Related Commands **config boot**

show 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 51
config 802.11 cac multimedia, on page 59
show cac voice stats, on page 6

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
8.3	This command was introduced.

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

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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, on page 87
config certificate lsc
show certificate lsc
show certificate summary, on page 11
show local-auth certificates, on page 22

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
8.3	This command was introduced.

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
show mobility group member
config mobility group member

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
8.3	This command was introduced.

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, on page 87
config certificate lsc
show certificate compatibility, on page 10
show local-auth certificates, on page 22

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
8.3	This command was introduced.

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 234

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*

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

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 [*ssid / ip / username / devicetype*]

Syntax Description

This command has no arguments or keywords.

Syntax Description

ssid / ip / username / devicetype	(Optional) Displays active clients selective details on any of the following parameters or all the parameters in any order: • SSID • IP addresss • Username • Device type (such as Samsung-Device or WindowsXP-Workstation)

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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 (blacklisted).

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
```

The following example shows how to display all clients that are WindowsXP-Workstation device type:

```
(Cisco Controller) >show client summary WindowsXP-Workstation
Number of Clients in WLAN....................... 0

MAC Address       AP Name    Status        Auth Protocol         Port Wired Mobility Role

----------------- -------- ------------- ----------------       ---------- --------------

Number of Clients with requested device type..... 0
```

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 **show custom-web** command.

show custom-web *all remote-lan guest-lan sleep-client webauth-bundle wlan*

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
8.3	This command was introduced.

The following is a sample output of the **show custom-web all** 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

Command History

Release	Modification
8.3	This command was introduced.

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 dtls connections

To display the Datagram Transport Layer Security (DTLS) server status, use the **show dtls connections** command.

show dtls connections

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following is a sample output of the **show dtls connections** command.

```
Device > show dtls connections

AP Name          Local Port    Peer IP         Peer Port     Ciphersuite
---------------- ------------- --------------- ------------- -----------------------
1130             Capwap_Ctrl   1.100.163.210   23678         TLS_RSA _WITH_AES_128_CBC_SHA
1130             Capwap_Data   1.100.163.210   23678         TLS_RSA _WITH_AES_128_CBC_SHA
1240             Capwap_Ctrl   1.100.163.209   59674         TLS_RSA _WITH_AES_128_CBC_SHA
```

show 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
	8.3	This command was introduced.

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
	8.3	This command was introduced.

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
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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 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.

Command History

Release	Modification
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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 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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to display a summary configuration:

```
(Cisco Controller) >show network summary
RF-Network Name............................. RF
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
Secure Web Mode RC4 Cipher Preference....... Disable
OCSP........................................ Disabled
OCSP responder URL..........................
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable   Mode: Ucast
Ethernet Broadcast Mode..................... Disable
Ethernet Multicast Forwarding............... Disable
Ethernet Broadcast Forwarding............... Disable
AP Multicast/Broadcast Mode................. Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
IGMP Query Interval......................... 20 seconds
MLD snooping................................ Disabled
MLD timeout................................. 60 seconds
MLD query interval.......................... 20 seconds
User Idle Timeout........................... 300 seconds
AP Join Priority............................ Disable
ARP Idle Timeout............................ 300 seconds
ARP Unicast Mode............................ Disabled
Cisco AP Default Master..................... Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Over The Air Provisioning of AP's........... Enable
Apple Talk ................................. Disable
Mesh Full Sector DFS........................ Enable
AP Fallback ................................ Disable
Web Auth CMCC Support ...................... Disabled
Web Auth Redirect Ports .................... 80
Web Auth Proxy Redirect  ................... Disable
Web Auth Captive-Bypass   .................. Disable
Web Auth Secure Web  ....................... Enable
Fast SSID Change ........................... Disabled
AP Discovery - NAT IP Only ................. Enabled
IP/MAC Addr Binding Check .................. Enabled
CCX-lite status ............................ Disable
oeap-600 dual-rlan-ports ................... Disable
oeap-600 local-network ..................... Enable
mDNS snooping............................... Disabled
mDNS Query Interval......................... 15 minutes
Web Color Theme............................. Red
Web Color Theme............................. Default
CAPWAP Prefer Mode.......................... IPv4
```

show 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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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
8.3	This command was introduced.

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 27
show nmsp statistics, on page 28
config nmsp notify-interval measurement, on page 139
clear nmsp statistics, on page 194
clear locp statistics, on page 192

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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 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.

Command History

Release	Modification
8.3	This command was introduced.

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 run-config

To display a comprehensive view of the current Cisco Mobility Express controller configuration, use the **show run-config all** command.

show run-config {**all** | **commands**} [**no-ap** | **commands**]

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
8.3	This command was introduced.

Usage Guidelines These commands have replaced the **show running-config** command.

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 **show run-config all** 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...
```

Related Topics

config passwd-cleartext, on page 141
show trapflags, on page 41

show run-config startup-commands

To display a comprehensive view of the current Cisco wireless LAN controller configuration, use the **showrun-configstartup-commands** command.

show run-configstartup-commands

Syntax Description

run-config	Displays the running configuration commands.
startup-commands	Display list of configured startup commands on Wireless LAN Controller.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The configuration commands on the Wireless LAN controller are uploaded to the TFTP or NCS servers using the transfer upload process. The **show run-config startup-commands** command enables the Wireless LAN controller to generate running-configuration in CLI format. The configuration commands generated can be used as backup configuration to restore the network.

Example

The following is a sample output of the **show run-config startup-commands** command:

show run-config startup-commands

```
(Cisco Controller) >show run-config
  startup-commands

(Cisco Controller) >show run-config startup-commands

This may take some time.
Are you sure you want to proceed? (y/N) y


config location expiry tags 5
config mdns profile service add default-mdns-profile AirPrint
config mdns profile service add default-mdns-profile AirTunes
config mdns profile service add default-mdns-profile AppleTV
config mdns profile service add default-mdns-profile HP_Photosmart_Printer_1
config mdns profile service add default-mdns-profile HP_Photosmart_Printer_2
config mdns profile service add default-mdns-profile Printer
config mdns profile create default-
```

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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 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

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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
8.3	This command was introduced.

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)
```

config Commands

This section lists the **config** commands that you can use to configure the controller settings, and manage user accounts.

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.
loud	Enables the 802.11h channel switch announcement in the loud mode. The 802.11h-enabled clients can send packets while switching channel.
quiet	Enables 802.11h-enabled clients to stop transmitting packets immediately because the AP has detected radar and client devices should also quit transmitting to reduce interference.
disable	Disables the 802.11h channel switch announcement.

Command Default None

Command History

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

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

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
8.3	This command was introduced.

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.

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
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.
- Enable call snooping on the WLAN on which the SIP client is present by entering the **config wlan call-snoop enable** *wlan_id* command.

Command History

Release	Modification
8.3	This command was introduced.

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).

Command History

Release	Modification
8.3	This command was introduced.

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.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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

Command Default

The transmission is enabled for the entire network by default.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

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

config 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
8.3	This command was introduced.

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 radioon slot 1 and 802.11ac on slot 2.
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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 rssi-check

To configure the 802.11 RSSI Low Check feature, use the **config 802.11 rssi-check** command.

config 802.11 {**a** | **b**} **rssi-check** {**enable** | **disable**}

Syntax Description

rssi-check	Configures the RSSI Low Check feature.
enable	Enables the RSSI Low Check feature.
disable	Disables the RSSI Low Check feature.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

config 802.11 rssi-threshold

To configure the 802.11 RSSI Low Check threshold, use the **config 802.11 rssi-threshold** command.

config 802.11 {**a** | **b**} **rssi-threshold** *value-in-dBm*

Syntax Description

rssi-threshold	Configures the RSSI Low Check threshold value.
value-in-dBm	RSSI threshold value in dBm. The default value is –80 dBm.

Command Default The default value of the RSSI Low Check threshold is –80 dBm.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines The following example shows how to configure the RSSI threshold value to –70 dBm for an 802.11a network:

```
(Cisco Controller) > config 802.11a rssi-threshold -70
```

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 radiusauth

To configure the RADIUS web authentication method, use the **config custom-web radiusauth** command.

config custom-web radiusauth {**chap** | **md5chap** | **pap**}

Syntax Description

chap	Configures the RADIUS web authentication method as Challenge Handshake Authentication Protocol (CHAP).
md5chap	Configures the RADIUS web authentication method as Message Digest 5 CHAP (MD5-CHAP).
pap	Configures the RADIUS web authentication method as Password Authentication Protocol (PAP).

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the RADIUS web authentication method as MD5-CHAP:

```
(Cisco Controller) > config custom-web radiusauth md5chap
```

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 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
8.3	This command was introduced.

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 sleep-client

To delete a web-authenticated sleeping client, use the **config custom-web sleep-client** command.

config custom-web sleep-client delete *mac_address*

Syntax Description

delete	Deletes a web-authenticated sleeping client with the help of the client MAC address.
mac_address	MAC address of the sleeping client.

Command Default

The web-authenticated sleeping client is not deleted.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to delete a web-authenticated sleeping client:

```
(Cisco Controller) > config custom-web sleep-client delete 0:18:74:c7:c0:90
```

Related Topics

config wlan custom-web
show custom-web, on page 18

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 22

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

The following example shows how to close all active Telnet sessions:

```
(Cisco Controller) > config loginsession close all
```

Related Commands

show loginsession

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

The following example shows how to add a description “master-user” to the management user “admin”:

```
(Cisco Controller) > config mgmtuser description admin "master 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
8.3	This command was introduced.

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 mgmtuser telnet

To enable local management users to use Telnet to connect to the Cisco Wireless LAN Controller, use the **config mgmtuser telnet** command.

config mgmtuser telnet *user_name* {**enable** | **disable**}

Syntax Description

user_name	Username of a local management user.
enable	Enables a local management user to use Telnet to connect to the Cisco WLC. You can enter up to 24 alphanumeric characters.
disable	Disables a local management user from using Telnet to connect to the Cisco WLC.

Command Default

Local management users can use Telnet to connect to the Cisco WLC.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

You must enable global Telnet to enable this command. Secure Shell (SSH) connection is not affected when you enable this option.

The following example shows how to enable a local management user to use Telnet to connect to the Cisco WLC:

```
(Cisco Controller) > config mgmtuser telnet admin1 enable
```

Related Topics

config mgmtuser add, on page 117
config mgmtuser delete, on page 118
config mgmtuser description, on page 118
config mgmtuser password, on page 119
show mgmtuser, on page 24

config mgmtuser termination-interval

To configure the user re-authentication terminal interval in seconds, use the **config mgmtuser termination-interval** command.

config mgmtuser termination-interval {*seconds* }

Syntax Description

seconds	Re-authentication terminal interval in seconds for a user before being logged out. Default value is 0, the valid range is 0 to 300 seconds.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to set the interval in seconds before the user is logged out:

```
(Cisco Controller) > config mgmtuser termination-interval 180
```

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
8.3	This command was introduced.

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** *username* | **wlan-id** *wlan-id* }

Syntax Description

username	Network username. The username can be up to 24 alphanumeric characters.
wlan-id	WLAN identification number.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines Local network usernames must be unique because they are stored in the same database.

Note When a WLAN associated with network users is deleted, the system prompts to delete all network users associated with the WLAN first. After deleting the network users, you can delete the WLAN.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

The following example shows how to enable the lightweight access point priority reauthorization:

```
(Cisco Controller) > config network ap-priority enable
```

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
8.3	This command was introduced.

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. 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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
```

Command History

Release	Modification
8.3	This command was introduced.

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
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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

Command History

Release	Modification
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 qos qosmap

To configure QoS map, use the **config qos qosmap** command.

config qos qosmap {**enable** | **disable** | **default** }

Syntax Description

enable	Enables the QoS map feature.
disable	Disables the QoS map feature.
default	Resets to default QoS map. This resets the QoS map values to 255 (default), and also adds DSCP UP exceptions if not present previously. To clear the DSCP UP values, enter the **config qos qosmap clear-all** command.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the QoS map.

```
(Cisco Controller) > config qos qosmap enable
```

config qos qosmap up-to-dscp-map

To configure the DSCP range for UP, use the **config qos qosmap** command.

config qos qosmap up-to-dscp-map {*up dscp-default dscp-start dscp-end*}

Syntax Description

up-to-dscp-map	Sets the DSCP range for UP
up	Wireless UP value
dscp-default	Default DSCP value for this UP
dscp-start	The DSCP start range. Range is between 0-63
dscp-end	The DSCP stop range. Range is 0-63

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to set the DSCP range for UP.

```
(Cisco Controller) > config qos qosmap up-to-dscp-map 2 3 5 20
```

config qos qosmap dscp-to-up-exception

To configure the DSCP exception, use the **config qos qosmap** command.

config qos qosmap dscp-to-up-exception {*dscp up* }

Syntax Description

dscp-to-up-exception	Allows to configure DSCP exception.
dscp	Exception DSCP value for the UP value
up	Links to the Wireless User Priority (UP) value

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the DSCP exception:

```
(Cisco Controller) > config qos qosmap dscp-to-up-exception 3 1
```

config qos qosmap delete-dscp-exception

To delete a dscp exception, use the **config qos qosmap** command.

config qos qosmap delete-dscp-exception *dscp*

Syntax Description

delete-dscp-exception	Deletes exception for DSCP
dscp	DSCP exception for the UP

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to delete a exception for DSCP.

```
(Cisco Controller) > config qos qosmap delete-dscp-exception 23
```

config qos qosmap clear-all

To delete all the exceptions from the QoS map, use the **config qos qosmap** command.

config qos qosmap clear-all

Syntax Description

clear-all	Deletes all the exceptions

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to clear all the exceptions from the QoS map.

```
(Cisco Controller) > config qos qosmap clear-all
```

config qos qosmap trust dscp upstream

To mark the upstream packets using the client dscp, use the **config qos qosmap** command.

config qos qosmap trust-dscp-upstream {**enable** | **disable** }

Syntax Description

trust-dscp-upstream	Based on the client's DSCP the upstream packets are marked
enable	Enables the upstream packet marking using the client dscp.
disable	Disables the upstream packet marking using the client dscp.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable client dscp based packet marking.

```
(Cisco Controller) > config qos qosmap trust-dscp-upstream enable
```

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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** | **position-check** | **case-digit-check** | **minimum** {**upper-case** | **lower-case** | **digits** | **special-chars**} *no._of_characters* | **min-length** | *password_length* | **lockout**{**mgmtuser** | **snmpv3user** | **time** | **attempts**} | **lifetime** {**mgmtuser** | **snmpv3user**} *lifetime* | **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.
position-check	Checks whether the password has a four-character change from the old password.
case-digit-check	Checks whether the password has all the four combinations: lower, upper, digits, or special characters.
minimum	Checks whether the password has a minimum number of upper case and lower case characters, digits, or special characters.

upper-case	Checks whether the password has a minimum number of upper case characters.
lower-case	Checks whether the password has a minimum number of lower case characters.
digits	Checks whether the password has a minimum number of digits.
special-chars	Checks whether the password has a minimum number of special characters.
min-length	Configures the minimum length for the password.
password_length	Minimum length for the password. The range is from 3 to 24 case-sensitive characters.
lockout	Configures the lockout feature for a management user or Simple Network Management Protocol version 3 (SNMPv3) user.
mgmtuser	Locks out a management user when the number of successive failed attempts exceed the management user lockout attempts.
snmpv3user	Locks out a SNMPv3 user when the number of successive failed attempts exceeds the SNMPv3 user lockout attempts.
time	Configures the time duration after the lockout attempts when the management user or SNMPv3 user is locked.
attempts	Configures the number of successive incorrect password attempts after which the management user or SNMPv3 user is locked.
lifetime	Configures the number of days before the management user or SNMPv3 user requires a change of password due to the age of the password.
mgmtuser	Configures the number of days before the management user requires a change of password due to the password age.
snmpv3user	Configures the number of days before the SNMPv3 user requires a change of password due to the age of the password.
lifetime	Number of days before the management user or SNMPv3 user requir*lifetime*es a change of password due to the age of the password.
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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 36
config snmp community accessmode, on page 153
config snmp community create, on page 153
config snmp community delete, on page 154
config snmp community mode, on page 155

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 37

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 40
show ntp-keys, on page 31

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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

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
8.3	This command was introduced.

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 39

Timeout Commands

This section lists the timeout commands of the controller:

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).

Command History

Release	Modification
8.3	This command was introduced.

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.

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.

Command History

Release	Modification
8.3	This command was introduced.

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
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

config 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.

Command History

Release	Modification
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
```

Clearing Configurations, Log files, and Other Actions

Use the **clear** command to clear existing configurations, log files, and other functions.

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
8.3	This command was introduced.

Usage Guidelines

Entering this command does not clear the static IP address of the access point.

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

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

clear ap eventlog

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

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

Syntax Description

specific	Specifies a specific access point log file.
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
8.3	This command was introduced.

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

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

clear ap join stats

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

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

Syntax Description

all	Specifies all access points.
ap_mac	Access point MAC address.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

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

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

clear 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
	8.3	This command was introduced.

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

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

Related Commands **show radius acct statistics**

clear session

To clear sessions that are created when user logs in through Telnet or SSH, use the **clear session** command.

clear session *session-id*

Command Default None

Command History	Release	Modification
	8.3	This command was introduced.

Usage Guidelines The session ID for clearing the session should be taken from the **show login-session** command.

The following example shows how to clear Telnet or SSH sesion:

```
(Cisco Controller) >clear session 3
```

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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

Resetting the System Reboot Time

Use the **reset** command to schedule a reboot of the controller and access points.

reset system at

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

Related Topics

reset system in, on page 205
reset system notify-time, on page 207

reset system in

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

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

Syntax Description

HH :MM :SS	Specifies a delay in duration.

image	Configures the image to be rebooted.
swap	Changes the active boot image; boots the non-active image and sets the default flag on it on the next reboot.
reset-aps	Resets all access points during the system reset.
save-config	Saves the configuration before the system reset.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

Related Topics

reset system at, on page 205
reset system notify-time, on page 207

reset system cancel

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

reset system cancel

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to cancel a scheduled reset:

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

Related Topics

reset system at, on page 205
reset system in, on page 205
reset system notify-time, on page 207

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
8.3	This command was introduced.

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

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

Related Topics

reset system at, on page 205
reset system in, on page 205

Uploading and Downloading Files and Configurations

Use the **transfer** command to transfer files to or from the Cisco Wireless LAN controller.

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
8.3	This command was introduced.

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 200
transfer download mode, on page 211
transfer download filename, on page 210
transfer download path, on page 212
transfer download serverip, on page 213
transfer download start, on page 214
transfer upload datatype, on page 218
transfer upload mode, on page 220
transfer upload filename, on page 219
transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224

transfer download datatype

To set the download file type, use the **transfer download datatype** command.

transfer download datatype {**avc-protocol-pack** | **code** | **config** | **eapdevcert** | **eapcacert** | **icon** | **image** | **ipseccacert** | **ipsecdevcert** | **login-banner** | **radius-avplist** | **signature** | **webadmincert** | **webauthbundle** | **webauthcert**}

Syntax Description

avc-protocol-pack	Downloads an AVC protocol pack to the system.
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.
radius-avplist	Downloads the RADIUS AVPs in the XML file format from the FTP server.
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
8.3	This command was introduced.

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 200
transfer download mode, on page 211
transfer download path, on page 212

transfer download serverip, on page 213
transfer download start, on page 214
transfer upload datatype, on page 218
transfer upload mode, on page 220
transfer upload filename, on page 219
transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224

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
8.3	This command was introduced.

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 200
transfer download certpasswor, on page 208
transfer download mode, on page 211
transfer download path, on page 212
transfer download serverip, on page 213
transfer download start, on page 214
transfer upload datatype, on page 218
transfer upload mode, on page 220
transfer upload filename, on page 219
transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224

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
8.3	This command was introduced.

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 200
transfer download filename, on page 210
transfer download certpasswor, on page 208
transfer download path, on page 212
transfer download serverip, on page 213
transfer download start, on page 214
transfer upload datatype, on page 218
transfer upload filename, on page 219
transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224

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
8.3	This command was introduced.

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 211
transfer download port, on page 213
transfer upload username, on page 225

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
8.3	This command was introduced.

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 200
transfer download mode, on page 211
transfer download certpasswor, on page 208
transfer download filename, on page 210
transfer download serverip, on page 213
transfer download start, on page 214
transfer upload datatype, on page 218
transfer upload mode, on page 220
transfer upload filename, on page 219

transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224

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.

ch

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to specify FTP port number 23:

```
(Cisco Controller) > transfer download port 23
```

Related Topics

transfer download mode, on page 211
transfer download path, on page 212
transfer download username, on page 216

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
8.3	This command was introduced.

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 200
transfer download mode, on page 211
transfer download filename, on page 210
transfer download path, on page 212
transfer download serverip, on page 213
transfer download start, on page 214
transfer upload datatype, on page 218
transfer upload mode, on page 220
transfer upload filename, on page 219
transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224

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
8.3	This command was introduced.

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 200
transfer download mode, on page 211
transfer download certpasswor, on page 208

transfer download filename, on page 210
transfer download path, on page 212
transfer download serverip, on page 213
transfer download password, on page 211
transfer upload datatype, on page 218
transfer upload mode, on page 220
transfer upload filename, on page 219
transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224

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
8.3	This command was introduced.

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 200
transfer download mode, on page 211
transfer download filename, on page 210
transfer download path, on page 212
transfer download serverip, on page 213
transfer download start, on page 214
transfer upload datatype, on page 218
transfer upload mode, on page 220
transfer upload filename, on page 219
transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224

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
8.3	This command was introduced.

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 200
transfer download mode, on page 211
transfer download filename, on page 210
transfer download path, on page 212
transfer download serverip, on page 213
transfer download start, on page 214
transfer upload datatype, on page 218
transfer upload mode, on page 220
transfer upload filename, on page 219
transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224

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
8.3	This command was introduced.

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 211
transfer download path, on page 212
transfer download password, on page 211

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
8.3	This command was introduced.

The following example shows how to enable the encryption settings:

```
(Cisco Controller) > transfer encrypt enable
```

Related Topics

clear transfer, on page 200
transfer download mode, on page 211
transfer download filename, on page 210
transfer download path, on page 212
transfer download serverip, on page 213
transfer download start, on page 214
transfer upload datatype, on page 218
transfer upload mode, on page 220
transfer upload filename, on page 219
transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224

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** | **ipseccacert** | **ipsecdevcert** | **pac** | **packet-capture** | **panic-crash-file** | **radio-core-dump** | **radius-avplist** | **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.
ipseccacert	Uploads CA certificate file.
ipsecdevcert	Uploads device certificate 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.
radius-avplist	Uploads the XML file from the controller to the RADIUS server.
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
8.3	This command was introduced.

The following example shows how to upload the system error log file:

```
(Cisco Controller) > transfer upload datatype errorlog
```

Related Topics

clear transfer, on page 200
transfer upload filename, on page 219
transfer upload mode, on page 220
transfer upload pac, on page 221
transfer upload password, on page 221
transfer upload path, on page 222
transfer upload port, on page 223
transfer upload serverip, on page 223
transfer upload start, on page 224
transfer upload username, on page 225

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
8.3	This command was introduced.

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 200
transfer upload datatype, on page 218
transfer upload mode, on page 220
transfer upload pac, on page 221
transfer upload password, on page 221
transfer upload path, on page 222
transfer upload port, on page 223
transfer upload serverip, on page 223
transfer upload start, on page 224
transfer upload username, on page 225

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
8.3	This command was introduced.

The following example shows how to set the transfer mode to TFTP:

```
(Cisco Controller) > transfer upload mode tftp
```

Related Topics

clear transfer, on page 200
transfer upload datatype, on page 218
transfer upload filename, on page 219
transfer upload pac, on page 221
transfer upload password, on page 221
transfer upload path, on page 222

transfer upload port, on page 223
transfer upload serverip, on page 223
transfer upload start, on page 224
transfer upload username, on page 225

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
8.3	This command was introduced.

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 200
transfer upload datatype, on page 218
transfer upload filename, on page 219
transfer upload mode, on page 220
transfer upload password, on page 221
transfer upload path, on page 222
transfer upload port, on page 223
transfer upload serverip, on page 223
transfer upload start, on page 224
transfer upload username, on page 225

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
8.3	This command was introduced.

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 200
transfer upload datatype, on page 218
transfer upload filename, on page 219
transfer upload mode, on page 220
transfer upload pac, on page 221
transfer upload port, on page 223
transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224
transfer upload username, on page 225

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
8.3	This command was introduced.

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 200
transfer upload datatype, on page 218
transfer upload filename, on page 219
transfer upload mode, on page 220
transfer upload pac, on page 221
transfer upload password, on page 221
transfer upload port, on page 223
transfer upload serverip, on page 223
transfer upload start, on page 224
transfer upload username, on page 225

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
8.3	This command was introduced.

The following example shows how to specify FTP port 23:

```
(Cisco Controller) > transfer upload port 23
```

Related Topics

clear transfer, on page 200
transfer upload datatype, on page 218
transfer upload filename, on page 219
transfer upload mode, on page 220
transfer upload pac, on page 221
transfer upload password, on page 221
transfer upload path, on page 222
transfer upload serverip, on page 223
transfer upload start, on page 224
transfer upload username, on page 225

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
8.3	This command was introduced.

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 200
transfer upload datatype, on page 218
transfer upload filename, on page 219
transfer upload mode, on page 220
transfer upload pac, on page 221
transfer upload password, on page 221
transfer upload path, on page 222
transfer upload port, on page 223
transfer upload start, on page 224
transfer upload username, on page 225

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
8.3	This command was introduced.

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 200
transfer upload datatype, on page 218
transfer upload filename, on page 219
transfer upload mode, on page 220
transfer upload pac, on page 221
transfer upload password, on page 221
transfer upload path, on page 222
transfer upload port, on page 223
transfer upload serverip, on page 223
transfer upload username, on page 225

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
8.3	This command was introduced.

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 200
transfer upload datatype, on page 218
transfer upload filename, on page 219
transfer upload mode, on page 220
transfer upload pac, on page 221
transfer upload password, on page 221
transfer upload path, on page 222
transfer upload port, on page 223
transfer upload serverip, on page 223

transfer upload start, on page 224

Troubleshooting the Controller Settings

This section describes the **debug** and **config** commands that you can use to troubleshoot the controller.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

The following example shows how to enable CDP event debugging in a Cisco controller:

```
(Cisco Controller) > debug cdp
```

Related Topics

config cdp, on page 86
show cdp, on page 9

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
8.3	This command was introduced.

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

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging of DHCP messages:

```
(Cisco Controller) >debug dhcp message 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
8.3	This command was introduced.

The following example shows how to disable all debug messages:

```
(Cisco Controller) > debug disable-all
```

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
8.3	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 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
8.3	This command was introduced.

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 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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

The following example shows how to enable the debugging of NTP settings:

```
(Cisco Controller) > debug ntp packet 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

Command History

Release	Modification
8.3	This command was introduced.

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

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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 115
config memory monitor leaks, on page 116
debug memory, on page 231

show run-config

To display a comprehensive view of the current Cisco Mobility Express controller configuration, use the **show run-config all** command.

show run-config {**all** | **commands**} [**no-ap** | **commands**]

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
8.3	This command was introduced.

Usage Guidelines

These commands have replaced the **show running-config** command.

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 **show run-config all** 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...
```

Related Topics

config passwd-cleartext, on page 141

show trapflags, on page 41

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.

Command History

Release	Modification
8.3	This command was introduced.

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.

Command History

Release	Modification
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
8.3	This command was introduced.

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
```

test aaa radius

To test AAA RADIUS interactions for WLAN authentication, use the **test aaa radius** command.

This test command sends to the RADIUS server an access request for client authentication. Access request exchange takes place between Cisco WLC and AAA server, and the registered RADIUS callback handles the response.

The response includes authentication status, number of retries, and RADIUS attributes.

test aaa radius username *username* **password** *password* **wlan-id** *wlan-id* [**apgroup** *apgroupname* **server-index** *server-index*]

Syntax Description

username	Username in plain text
password	Password in plain text
wlan-id	WLAN ID
apgroupname	AP group name (Optional)
server-index	AAA server index (Optional)

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

- Both username and password must be plain text, similar to MAC authentication
- If AP group is entered, the WLAN entered must belong to that AP group
- If server index is entered, the request to test RADIUS is sent only to that RADIUS server
- If the RADIUS request does not get a response, the request is not sent to any other RADIUS server
- RADIUS server at the server index must be in enabled state
- This test command can be used to verify configuration and communication related to AAA RADIUS server and should not be used for actual user authentication
- It is assumed that the AAA server credentials are set up as required

This example shows a scenario where access is accepted:

```
(Cisco Controller) > test aaa radius username user1 password Cisco123 wlan-id 7 apgroup
default-group server-index 2

Radius Test Request

  Wlan-id..................................... 7
  ApGroup Name................................ default-group

  Attributes                      Values
  ----------                      ------
  User-Name                       user1
  Called-Station-Id               00:00:00:00:00:00:EngineeringV81
  Calling-Station-Id              00:11:22:33:44:55
  Nas-Port                        0x0000000d (13)
  Nas-Ip-Address                  172.20.227.39
  NAS-Identifier                  WLC5520
  Airespace / WLAN-Identifier     0x00000007 (7)
  User-Password                   Cisco123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x00000051 (81)
  Cisco / Audit-Session-Id        ac14e327000000c456131b33
  Acct-Session-Id                 56131b33/00:11:22:33:44:55/210

test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) > test aaa show radius

Radius Test Request
  Wlan-id..................................... 7
  ApGroup Name................................ default-group
  Server Index................................ 2
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
172.20.227.52            1     Success
Authentication Response:
  Result Code: Success
  Attributes                      Values
  ----------                      ------
  User-Name                       user1
  Class                           CACS:rs-acs5-6-0-22/230677882/20313
  Session-Timeout                 0x0000001e (30)
  Termination-Action              0x00000000 (0)
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x00000051 (81)

(Cisco Controller) > debug aaa all enable

*emWeb: Oct 06 09:48:12.931: 00:11:22:33:44:55 Sending Accounting request (2) for station
00:11:22:33:44:55
*emWeb: Oct 06 09:48:12.932: 00:11:22:33:44:55 Created Cisco-Audit-Session-ID for the mobile:

ac14e327000000c85613fb4c
*aaaQueueReader: Oct 06 09:48:12.932: User user1 password lengths don't match
*aaaQueueReader: Oct 06 09:48:12.932: ReProcessAuthentication previous proto 8, next proto
 40000001
*aaaQueueReader: Oct 06 09:48:12.932: AuthenticationRequest: 0x2b6d5ab8
*aaaQueueReader: Oct 06 09:48:12.932:  Callback.....................................0x101cd740
*aaaQueueReader: Oct 06 09:48:12.932:  protocolType.................................0x40000001
```

```
*aaaQueueReader: Oct 06 09:48:12.932:  proxyState.....................00:11:22:33:44:55-00:00
*aaaQueueReader: Oct 06 09:48:12.932:  Packet contains 16 AVPs (not shown)
*aaaQueueReader: Oct 06 09:48:12.932: Putting the quth request in qid 5, srv=index 1
*aaaQueueReader: Oct 06 09:48:12.932: Request
Authenticator 3c:b3:09:34:95:be:ab:16:07:4a:7f:86:3b:58:77:26
*aaaQueueReader: Oct 06 09:48:12.932: 00:11:22:33:44:55 Sending the packet
to v4 host 172.20.227.52:1812
*aaaQueueReader: Oct 06 09:48:12.932: 00:11:22:33:44:55 Successful transmission of
Authentication Packet (id 13) to 172.20.227.52:1812 from server queue 5,
proxy state 00:11:22:33:44:55-00:00
. . .
*radiusTransportThread: Oct 06 09:48:12.941: 00:11:22:33:44:55 Access-Accept received from

RADIUS server 172.20.227.52 for mobile 00:11:22:33:44:55 receiveId = 0
*radiusTransportThread: Oct 06 09:48:12.941: AuthorizationResponse: 0x146c56b8
*radiusTransportThread: Oct 06 09:48:12.941: structureSize.............................263
*radiusTransportThread: Oct 06 09:48:12.941: resultCode.................................0
*radiusTransportThread: Oct 06 09:48:12.941:
protocolUsed.................................0x00000001
*radiusTransportThread: Oct 06 09:48:12.941:
proxyState.....................00:11:22:33:44:55-00:00
*radiusTransportThread: Oct 06 09:48:12.941: Packet contains 7 AVPs:
*radiusTransportThread: Oct 06 09:48:12.941: AVP[01] User-Name.................user1 (5
bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[02]
Class..........CACS:rs-acs5-6-0-22/230677882/20696 (35 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[03] Session-Timeout........0x0000001e (30)
 (4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[04] Termination-Action....0x00000000 (0)
(4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[05] Tunnel-Type......0x0100000d (16777229)
 (4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[06] Tunnel-Medium-Type...0x01000006
(16777222) (4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[07] Tunnel-Group-Id.......DATA (3 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: Received radius callback for
test aaa radius request result 0 numAVPs 7.
```

Related Topics

test aaa show radius, on page 248

test aaa show radius

To view the RADIUS response to test RADIUS request, use the **test aaa show radius** command.

test aaa show radius

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.