Cisco Mobility Express Command Reference, Cisco Wireless Release 8.10

First Published: 2019-10-19

Last Modified: 2022-03-04

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

This preface describes the audience, organization, and conventions of the *Cisco Mobility Express Command Reference Guide*. Cisco Mobility Express only supports the AireOS commands mentioned in this document. It also provides information on how to obtain other documentation.

This preface includes the following sections:

Audience

This publication is for experienced network administrators who configure and maintain Cisco wireless controllers and Cisco lightweight access points (Cisco APs).

Note Usage of **test** commands may cause system disruption such as an unexpected reboot of the controller. Therefore, we recommend that you use the **test** commands on controllers for debugging purposes with the help of Cisco Technical Assistance Center (TAC) personnel.

Document Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.

Convention	Indication
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means the following information will help you solve a problem.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.")

Warning Title	Description
Waarschuwing	Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)
Varoitus	Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)

Warning Title	Description
Attention	Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).
Warnung	Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)
Avvertenza	Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).
Advarsel	Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)
Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").
¡Advertencia!	Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")
Varning	Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

Related Documentation

These documents provide complete information about the Cisco Mobility Express solution:

- *Cisco Mobility Express User Guide*
- *Cisco Mobility Express Best Practices Guide*
- *Cisco Mobility Express Solution Release Notes*

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Using the Command-Line Interface

This chapter contains the following topics:

CLI Command Keyboard Shortcuts

The table below lists the CLI keyboard shortcuts to help you enter and edit command lines on the controller.

Table 1: CLI Command Keyboard Shortcuts

Action	Description	Keyboard Shortcut
Change	The word at the cursor to lowercase.	Esc I
	The word at the cursor to uppercase.	Esc u
Delete	A character to the left of the cursor.	Ctrl-h, Delete, or Backspace
	All characters from the cursor to the beginning of the line.	Ctrl-u
	All characters from the cursor to the end of the line.	Ctrl-k
	All characters from the cursor to the end of the word.	Esc d
	The word to the left of the cursor.	Ctrl-w or Esc Backspace
Display MORE output	Exit from MORE output.	q, Q, or Ctrl-C
	Next additional screen. The default is one screen. To display more than one screen, enter a number before pressing the Spacebar key.	Spacebar
	Next line. The default is one line. To display more than one line, enter the number before pressing the Enter key.	Enter
Enter or Return key character.		Ctrl-m
Expand the command or abbreviation.		Ctrl-t or Tab
Move the cursor	One character to the left (back).	Ctrl-b or Left Arrow
	One character to the right (forward).	Ctrl-f or Right Arrow
	One word to the left (back), to the beginning of the current or previous word.	Esc b
	One word to the right (forward), to the end of the current or next word.	Esc f
	To the beginning of the line.	Ctrl-a
	To the end of the line.	Ctrl-e
Redraw the screen at the prompt.		Ctrl-l or Ctrl-r

Action	Description	Keyboard Shortcut
Return to the EXEC mode from any configuration mode		Ctrl-z
Return to the previous mode or exit from the CLI from Exec mode.		exit command
Transpose a character at the cursor with a character to the left of the cursor.		Ctrl-t

Using the Interactive Help Feature

The question mark (?) character allows you to get the following type of help about the command at the command line. The table below lists the interactive help feature list.

Table 2: Interactive Help Feature List

Command	Description
help	Provides a brief description of the Help feature in any command mode.
? at the command prompt	Lists all commands available for a particular command mode.
partial command?	Provides a list of commands that begin with the character string.
partial command<Tab>	Completes a partial command name.
command ?	Lists the keywords, arguments, or both associated with a command.
command keyword ?	Lists the arguments that are associated with the keyword.

Using the help Command

Before you begin

To look up keyboard commands, use the help command at the root level.

help

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must back up until entering a '?' shows the available options. Two types of help are available:

1. Full help is available when you are ready to enter a command argument (for example show ?) and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example show pr?).

Example:

```
> help
HELP:
Special keys:
  DEL, BS... delete previous character
  Ctrl-A  .... go to beginning of line
  Ctrl-E  .... go to end of line
  Ctrl-F  .... go forward one character
  Ctrl-B  .... go backward one character
  Ctrl-D  .... delete current character
  Ctrl-U, X. delete to beginning of line
  Ctrl-K  .... delete to end of line
```

```
Ctrl-W  .... delete previous word
Ctrl-T  .... transpose previous character
Ctrl-P  .... go to previous line in history buffer
Ctrl-N  .... go to next line in history buffer
Ctrl-Z  .... return to root command prompt
Tab, <SPACE> command-line completion
Exit    .... go to next lower command prompt
?       .... list choices
```

Using the ? command

Before you begin

To display all of the commands in your current level of the command tree, or to display more information about a particular command, use the ? command.

command name **?**

When you enter a command information request, put a space between the **command name** and **?**.

Examples

This command shows you all the commands and levels available from the root level.

```
> ?
clear          Clear selected configuration elements.
config         Configure switch options and settings.
debug          Manages system debug options.
help           Help
linktest       Perform a link test to a specified MAC address.
logout         Exit this session. Any unsaved changes are lost.
ping           Send ICMP echo packets to a specified IP address.
reset          Reset options.
save           Save switch configurations.
show           Display switch options and settings.
transfer       Transfer a file to or from the switch.
```

Using the partial? command

Before you begin

To provide a list of commands that begin with the character string, use the partial command ?.

partial command?

There should be no space between the command and the question mark.

This example shows how to provide a command that begin with the character string “ad”:

```
> controller> config>ad?
```

The command that matches with the string “ad” is as follows:

```
advanced
```

Using the partial command<tab>

Before you begin

To completes a partial command name, use the partial command<tab> command.

partial command<tab>

There should be no space between the command and <tab>.

This example shows how to complete a partial command name that begin with the character string “cert”:

```
Controller >config>cert<tab> certificate
```

Using the command ?

Examples

To list the keywords, arguments, or both associated with the command, use the command ?.

command-name ?

There should be a space between the command and the question mark.

This example shows how to list the arguments and keyword for the command acl:

```
Controller >config acl ?
```

Information similar to the following appears:

```
apply          Applies the ACL to the data path.
counter        Start/Stop the ACL Counters.
create         Create a new ACL.
delete         Delete an ACL.
rule           Configure rules in the ACL.
cpu            Configure the CPU ACL Information
```

command keyword ?

To list the arguments that are associated with the keyword, use the command keyword ?:

command keyword ?

There should be space between the keyword and the question mark.

This example shows how to display the arguments associated with the keyword cpu:

```
Controller >config acl cpu ?
```

Information similar to the following appears:

```
none           None - Disable the CPU ACL
<name>         <name> - Name of the CPU ACL
```

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 58
config 802.11 cac multimedia, on page 66
show cac voice stats, on page 12

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 95
config certificate lsc
show certificate lsc
show certificate summary, on page 17
show local-auth certificates, on page 28

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
config mobility group member
show 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 95
config certificate lsc
show certificate compatibility, on page 16
show local-auth certificates, on page 28

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 239

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.

Usage Guidelines

This command provides the following information:

- The time when the report was received
- The MAC address of the access point to which the client is currently associated
- The MAC address of the access point to which the client was previously associated
- The channel of the access point to which the client was previously associated
- The SSID of the access point to which the client was previously associated
- The time when the client disassociated from the previous access point

- The reason for the client roam

Note For non-CCXv4 clients, the Layer 2 roam reason is not displayed in the command output. For more information, see CSCvv85022.

Examples

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.

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 34
show nmsp statistics, on page 35
config nmsp notify-interval measurement, on page 146
clear nmsp statistics, on page 200
clear locp statistics, on page 198

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

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 147
show trapflags, on page 47

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 controller 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 channe
quiet	Enables 802.11h-enabled clients to stop transmitting packets immediate 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

Usage Guidelines Cisco Catalyst 9120AXE, 9120AXP, and Cisco Catalyst 9130AXE access points should have at least two antennas configured if you want to disable this configuration.

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, on page 685

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/ax 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/ax 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 defa
custom	Configures custom Layer 2 client roaming RF paramet
min_rssi	Minimum received signal strength indicator (RSSI) tha associate to the access point. If the client's average rece threshold, reliable communication is usually impossible and roamed to another access point with a stronger signa is reached. The valid range is –80 to –90 dBm, and the
roam_hyst	How much greater the signal strength of a neighboring the client to roam to it. This parameter is intended to re between access points if the client is physically located two access points. The valid range is 2 to 4 dB, and the
scan_thresh	Minimum RSSI that is allowed before the client should When the RSSI drops below the specified value, the clie access point within the specified transition time. This para method to minimize the time that the client spends in a example, the client can scan slowly when the RSSI is ab rapidly when the RSSI is below the threshold. The vali the default value is –72 dBm.

trans_time	Maximum time allowed for the client to detect a suitable nei to and to complete the roam, whenever the RSSI from the c is below the scan threshold. The valid range is 1 to 10 secc 5 seconds. **Note** For high-speed client roaming applications in we recommend that you set the transition time

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, on page 717
config advanced 802.11 channel update, on page 714

config advanced sae anti-clog-threshold

To configure Simultaneous Authentication of Equals (SAE) anticlog threshold, use the **config advanced sae anti-clog-threshold** command.

config advanced sae anti-clog-threshold *limit*

Syntax Description

limit	Anticlogging enable threshold limit in terms of SAE block. Valid range is 0 to 90.

Command Default None

Command History

Release	Modification
8.10	This command was introduced.

The following example shows how to configure anticlogging threshold limit to a value of 10:

```
(Cisco Controller) > config advanced sae anti-clog-threshold 10
```

config advanced sae max-retry

To configure the maximum number of retries for a Simultaneous Authentication of Equals (SAE) message, use the **config advanced sae max-retry** command.

config advanced sae max-retry *limit*

Syntax Description		
	limit	Maximum number of retransmission attempts for an SAE message. Valid range is 2 to 4.

Command Default None

Command History

Release	Modification
8.10	This command was introduced.

The following example shows how to configure 4 as the maximum number of retries for an SAE message:

```
(Cisco Controller) > config advanced sae max-retry 4
```

config advanced sae retry-timeout

To configure the timeout period for a Simultaneous Authentication of Equals (SAE) message, use the **config advanced sae retry-timeout** command.

config advanced sae retry-timeout *timeout*

Syntax Description		
	timeout	SAE message retry timeout. Valid range is 200 to 2000 milliseconds.

Command Default None

Command History

Release	Modification
8.10	This command was introduced.

The following example shows how to configure a timeout period of 400 milliseconds for an SAE message:

```
(Cisco Controller) > config advanced sae retry-timeout 400
```

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

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 t 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, on page 467
show custom-web, on page 24

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 controller.
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 29

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 clien • 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 “primary-user” to the management user “admin”:

```
(Cisco Controller) > config mgmtuser description admin "primary-user"
```

Related Commands

config mgmtuser add

config mgmtuser delete

config mgmtuser password

show mgmtuser

config mgmtuser password

To configure a management user password, use the **config mgmtuser password** command.

config mgmtuser password *username password*

Syntax Description

username	Account username. The username can be up to 24 alphanumeric characters.
password	Account password. The password can be up to 24 alphanumeric characters.

Command Default

None

Command History

Release	Modification
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 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 controller. You can enter up to 24 alphanumeric characters.
disable	Disables a local management user from using Telnet to connect to the controller.

Command Default

Local management users can use Telnet to connect to the controller.

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 controller:

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

Related Topics

config mgmtuser add, on page 124
config mgmtuser delete, on page 125
config mgmtuser description, on page 125
config mgmtuser password, on page 126
show mgmtuser, on page 31

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 secureweb hsts

To enable or disable HSTS policy on the controller, use the **config network secureweb** command.

config network secureweb hsts { **enable** | **disable** }

Syntax Description

enable	Enables the HSTS policy on the controller.
disable	Disables the HSTS policy on the controller.

Command Default The HSTS policy is disabled by default.

Command History

Release	Modification
8.10.171.0	This command was introduced.

Usage Guidelines This command allows access the controller GUI over a client supporting HTTPS protocol only. The maximum time when enabled on the controller is one year.

The following example shows how to enable the HSTS policy on the controller:

```
(Cisco Controller) > config network secureweb hsts enable
```

Related Commands

config network secureweb cipher-option

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 controller 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 controller 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 controller.
disable	Disables a strong password check for the access point and controller.

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 42
config snmp community accessmode, on page 159
config snmp community create, on page 160
config snmp community delete, on page 160
config snmp community mode, on page 162

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 44

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 trapreceiver snmpv3

To configure SNMPv3 for a trap receiver, use the **config snmp trapreceiver snmpv3** command.

config snmp trapreceiver snmpv3 {**enable** *trap-receiver-name* **v3user** *v3-username* | {**disable** *trap-receiver-name*}

Syntax Description

enable	Enables SNMPv3 for the SNMP trap receiver.
trap-receiver-name	Name of the SNMP trap receiver.
v3user *v3-username*	Name of the SNMPv3 user that has to be mapped to the SNMP trap receiver.
disable	Disables SNMPv3 for the SNMP trap receiver.

Command Default

Command History

Release	Modification
8.10	This command was introduced.

Usage Guidelines

It is not possible to delete an SNMPv3 user profile if the user profile is mapped to an SNMP trap receiver.

The following example shows how to enable SNMPv3 for an SNMP trap receiver named *snmpv3-trap-receiver* and map it to an SNMPv3 username *snmpv3-user*:

```
(Cisco Controller) > config snmp trapreceiver snmpv3 enable snmpv3-trap-receiver v3user
snmpv3-user
```

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 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 an NTP server:

```
(Cisco Controller) > config time ntp delete 1
```

Related Topics

show time, on page 46
show ntp-keys, on page 38

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

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags mesh

config trapflags strong-pwdcheck

config trapflags rfid

config trapflags rogueap

show trapflags

config trapflags ap

To enable or disable the sending of Cisco lightweight access point traps, use the **config trapflags ap** command.

config trapflags ap {**register** | **interfaceUp**} {**enable** | **disable**}

Syntax Description

register	Enables sending a trap when a Cisco lightweight access point registers with Cisco switch.
interfaceUp	Enables sending a trap when a Cisco lightweight access point interface (A or B) comes up.
enable	Enables sending access point-related traps.
disable	Disables sending access point-related traps.

Command Default

By default, the sending of Cisco lightweight access point traps is enabled.

Command History

Release	Modification
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 45

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 controller 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 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
```

Related Commands **config tacacs athr**

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 controller) and you must remove the current LWAPP private configuration by using the **clear lwapp private-config** command.

Note The access point must be running Cisco 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 211
reset system notify-time, on page 212

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 211
reset system notify-time, on page 212

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 211
reset system in, on page 211
reset system notify-time, on page 212

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 211
reset system in, on page 211

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 206
transfer download mode, on page 216
transfer download filename, on page 216
transfer download path, on page 218
transfer download serverip, on page 219
transfer download start, on page 220
transfer upload datatype, on page 223
transfer upload mode, on page 226
transfer upload filename, on page 225
transfer upload path, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230

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 206
transfer download mode, on page 216
transfer download path, on page 218
transfer download serverip, on page 219

transfer download start, on page 220
transfer upload datatype, on page 223
transfer upload mode, on page 226
transfer upload filename, on page 225
transfer upload path, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230

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 206
transfer download certpasswor, on page 214
transfer download mode, on page 216
transfer download path, on page 218
transfer download serverip, on page 219
transfer download start, on page 220
transfer upload datatype, on page 223
transfer upload mode, on page 226
transfer upload filename, on page 225
transfer upload path, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230

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 206
transfer download filename, on page 216
transfer download certpasswor, on page 214
transfer download path, on page 218
transfer download serverip, on page 219
transfer download start, on page 220
transfer upload datatype, on page 223
transfer upload filename, on page 225
transfer upload path, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230

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 216
transfer download port, on page 219
transfer upload username, on page 231

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 206
transfer download mode, on page 216
transfer download certpasswor, on page 214
transfer download filename, on page 216
transfer download serverip, on page 219
transfer download start, on page 220
transfer upload datatype, on page 223
transfer upload mode, on page 226
transfer upload filename, on page 225
transfer upload path, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230

transfer download port

To specify the FTP port, use the **transfer download port** command.

transfer download port *port*

Syntax Description

port	FTP port.

Command Default

The default FTP *port* is 21.

Command History

Release	Modification
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 216
transfer download path, on page 218
transfer download username, on page 222

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 206

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 206
transfer download mode, on page 216
transfer download certpasswor, on page 214
transfer download filename, on page 216
transfer download path, on page 218
transfer download serverip, on page 219
transfer download password, on page 217
transfer upload datatype, on page 223

transfer upload mode, on page 226
transfer upload filename, on page 225
transfer upload path, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230

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 206
transfer download mode, on page 216
transfer download filename, on page 216
transfer download path, on page 218
transfer download serverip, on page 219
transfer download start, on page 220
transfer upload datatype, on page 223
transfer upload mode, on page 226
transfer upload filename, on page 225
transfer upload path, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230

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 206
transfer download mode, on page 216
transfer download filename, on page 216
transfer download path, on page 218
transfer download serverip, on page 219
transfer download start, on page 220
transfer upload datatype, on page 223
transfer upload mode, on page 226
transfer upload filename, on page 225
transfer upload path, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230

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 216
transfer download path, on page 218
transfer download password, on page 217

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 206
transfer download mode, on page 216
transfer download filename, on page 216
transfer download path, on page 218
transfer download serverip, on page 219
transfer download start, on page 220
transfer upload datatype, on page 223
transfer upload mode, on page 226
transfer upload filename, on page 225
transfer upload path, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230

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-file webadmincert** | **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 controller'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 206
transfer upload filename, on page 225
transfer upload mode, on page 226
transfer upload pac, on page 226
transfer upload password, on page 227
transfer upload path, on page 228
transfer upload port, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230
transfer upload username, on page 231

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 206
transfer upload datatype, on page 223
transfer upload mode, on page 226
transfer upload pac, on page 226
transfer upload password, on page 227
transfer upload path, on page 228
transfer upload port, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230

transfer upload username, on page 231

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 206
transfer upload datatype, on page 223
transfer upload filename, on page 225
transfer upload pac, on page 226
transfer upload password, on page 227
transfer upload path, on page 228
transfer upload port, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230
transfer upload username, on page 231

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 206
transfer upload datatype, on page 223
transfer upload filename, on page 225
transfer upload mode, on page 226
transfer upload password, on page 227
transfer upload path, on page 228
transfer upload port, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230
transfer upload username, on page 231

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 206
transfer upload datatype, on page 223
transfer upload filename, on page 225

transfer upload mode, on page 226
transfer upload pac, on page 226
transfer upload port, on page 228
transfer upload path, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230
transfer upload username, on page 231

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 206
transfer upload datatype, on page 223
transfer upload filename, on page 225
transfer upload mode, on page 226
transfer upload pac, on page 226
transfer upload password, on page 227
transfer upload port, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230
transfer upload username, on page 231

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 206
transfer upload datatype, on page 223
transfer upload filename, on page 225
transfer upload mode, on page 226
transfer upload pac, on page 226
transfer upload password, on page 227
transfer upload path, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230
transfer upload username, on page 231

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 206
transfer upload datatype, on page 223
transfer upload filename, on page 225
transfer upload mode, on page 226
transfer upload pac, on page 226
transfer upload password, on page 227
transfer upload path, on page 228
transfer upload port, on page 228
transfer upload start, on page 230
transfer upload username, on page 231

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 206
transfer upload datatype, on page 223
transfer upload filename, on page 225
transfer upload mode, on page 226
transfer upload pac, on page 226
transfer upload password, on page 227
transfer upload path, on page 228
transfer upload port, on page 228
transfer upload serverip, on page 229
transfer upload username, on page 231

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 206
transfer upload datatype, on page 223
transfer upload filename, on page 225
transfer upload mode, on page 226
transfer upload pac, on page 226
transfer upload password, on page 227
transfer upload path, on page 228
transfer upload port, on page 228
transfer upload serverip, on page 229
transfer upload start, on page 230

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 94
show cdp, on page 15

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 controller, 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 controller 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  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 122
config memory monitor leaks, on page 123

debug memory, on page 236

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

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 147
show trapflags, on page 47

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 controller 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 controller 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 253

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.

Ports and Interfaces Commands

show Commands

This section lists the **show** commands that you can use to display information about the controller ports and interfaces.

show interface summary

To display summary details of the system interfaces, use the **show interface summary** command.

show interface summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example displays the summary of the local IPv4 interfaces:

```
(Cisco Controller) > show interface summary
Number of Interfaces..... 6

Interface Name                  Port Vlan Id  IP Address      Type    Ap Mgr Guest
------------------------------- ---- -------- --------------- ------- ------ -----
dyn59                           LAG  59       9.10.59.66      Dynamic No     No
management                      LAG  56       9.10.56.60      Static  Yes    No
redundancy-management           LAG  56       0.0.0.0         Static  No     No
redundancy-port                 -    untagged 0.0.0.0         Static  No     No
service-port                    N/A  N/A      2.2.2.2         Static  No     No
virtual                         N/A  N/A      1.2.3.4         Static  No     No
```

The following example displays the summary of the local IPv6 interfaces:

```
show ipv6 interface summary
Number of Interfaces..... 2

Interface Name          Port Vlan Id  IPv6 Address/Prefix Length
----------------------- ---- -------- -----------------------------------------
management              LAG  56                    fe80::224:97ff:fe69:69af/64
                        LAG  56                           2001:9:10:56::60/64
service-port            N/A  N/A                   fe80::224:97ff:fe69:69a1/64
                        N/A  N/A                                       ::/128
```

show interface detailed

To display details of the system interfaces, use the **show interface** command.

show interfacedetailed {*interface_name* | **management** | **redundancy-management** | **redundancy-port** | **service-port** | **virtual**}

Syntax Description

detailed	Displays detailed interface information.
interface_name	Interface name for detailed display.
management	Displays detailed management interface information.
redundancy-management	Displays detailed redundancy management interface information.
redundancy-port	Displays detailed redundancy port information.
service-port	Displays detailed service port information.
virtual	Displays detailed virtual gateway interface information.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the detailed interface information:

```
(Cisco Controller) > show interface detailed management

Interface Name................................. management
MAC Address.................................... 00:24:97:69:69:af
IP Address..................................... 9.10.56.60
IP Netmask..................................... 255.255.255.0
IP Gateway..................................... 9.10.56.1
External NAT IP State.......................... Disabled
External NAT IP Address........................ 0.0.0.0
Link Local IPv6 Address........................ fe80::224:97ff:fe69:69af/64
STATE ......................................... REACHABLE
Primary IPv6 Address........................... 2001:9:10:56::60/64
STATE ......................................... REACHABLE
Primary IPv6 Gateway........................... fe80::aea0:16ff:fe4f:2242
Primary IPv6 Gateway Mac Address............... ac:a0:16:4f:22:42
STATE ......................................... REACHABLE
VLAN........................................... 56
Quarantine-vlan................................ 0
NAS-Identifier................................. Building1
Active Physical Port........................... LAG (13)
Primary Physical Port.......................... LAG (13)
Backup Physical Port........................... Unconfigured
DHCP Proxy Mode................................ Global
Primary DHCP Server............................ 9.1.0.100
Secondary DHCP Server.......................... Unconfigured
DHCP Option 82................................. Disabled
DHCP Option 82 bridge mode insertion.............. Disabled
IPv4 ACL....................................... Unconfigured
IPv6 ACL....................................... Unconfigured
mDNS Profile Name.............................. Unconfigured
```

```
AP Manager..................................... Yes
Guest Interface................................ No
L2 Multicast................................... Enabled
```

Note Some WLAN controllers may have only one physical port listed because they have only one physical port.

The following example shows how to display the detailed redundancy management interface information:

```
(Cisco Controller) > show interface detailed redundancy-management
Interface Name................................. redundancy-management
MAC Address.................................... 88:43:e1:7e:0b:20
IP Address..................................... 209.165.201.2
```

The following example shows how to display the detailed redundancy port information:

```
(Cisco Controller) > show interface detailed redundancy-port
Interface Name................................. redundancy-port
MAC Address.................................... 88:43:e1:7e:0b:22
IP Address..................................... 169.254.120.5
```

The following example shows how to display the detailed service port information:

```
(Cisco Controller) > show interface detailed service-port
Interface Name................................. redundancy-port
MAC Address.................................... 88:43:e1:7e:0b:22
IP Address..................................... 169.254.120.5
```

The following example shows how to display the detailed virtual gateway interface information:

```
(Cisco Controller) > show interface detailed virtual
Interface Name................................. virtual
MAC Address.................................... 88:43:e1:7e:0b:20
IP Address..................................... 192.0.2.1
Virtual DNS Host Name.......................... Disabled
AP Manager..................................... No
Guest Interface................................ No
```

Related Topics

config interface address, on page 263
show interface group

show port

To display the Cisco wireless controller port settings on an individual or global basis, use the **show port** command.

show port { *port-number* | **summary** | **detailed-info** | **sfp-info** | **vlan** }

Syntax Description

port-number	Port number of the physical interface.
summary	Displays a summary of all ports.
detailed-info	Displays detailed port information.
sfp-info	Displays SFP information. **Note** This feature is applicable only to Cisco 5520 and 8540 controllers.
vlan	Displays VLAN port table summary.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display information about an individual controller port:

```
(Cisco Controller) > show port 1                STP   Admin   Physical   Physical
  Link   Link    Mcast
Pr  Type   Stat   Mode     Mode      Status   Status  Trap   Appliance
 POE
-- ------- ---- ------- ---------- ---------- ------ ------- ---------
-------
1  Normal  Disa Enable  Auto       1000 Full  Down   Enable  Enable
N/A
```

Note Some controllers may not have multicast or Power over Ethernet (PoE) listed because they do not support those features.

The following example shows how to display a summary of all ports:

```
(Cisco Controller) > show port summary              STP   Admin   Physical
Physical   Link   Link    Mcast
Pr  Type   Stat   Mode     Mode      Status   Status  Trap   Appliance
 POE SFPType
-- ------- ---- ------- ---------- ---------- ------ ------- ---------
-------------
1  Normal  Forw Enable  Auto       1000 Full  Up     Enable  Enable
N/A NotPresent
2  Normal  Disa Enable  Auto       1000 Full  Down   Enable  Enable
N/A NotPresent
```

```
3  Normal  Disa Enable  Auto       1000 Full  Down   Enable  Enable
N/A NotPresent
4  Normal  Disa Enable  Auto       1000 Full  Down   Enable  Enable
N/A NotPresent
```

Note Some controllers may have only one port listed because they have only one physical port.

The following example shows how to display SFP information:

```
(Cisco Controller) > show port sfp-info (Cisco Controller) > FP0 Port SFP Vendor
  Transceiver Type    OUI PartNumber       Rev  SerialNumber     DateCode
 Auth
   1 CISCO-AVAGO      (0x08)1000BaseTX        XXXX-XXXXX
XXXXXXXXXXX      XXXXXX   ok
   2 Not Present      (0x00)NOT_SUPPORTED
                     fail
FP0.
```

Related Topics

- show stats port
- show stats switch
- config interface port
- config spanningtree port mode
- config spanningtree port pathcost
- config spanningtree port priority

show serial

To display the serial (console) port configuration, use the **show serial** command.

show serial

Syntax Description

This command has no arguments or keywords.

Command Default

The default values for Baud rate, Character, Flow Control, Stop Bits, Parity type of the port configuration are 9600, 8, off, 1, none.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display EIA-232 parameters and the serial port inactivity timeout:

```
(Cisco Controller) > show serial
Serial Port Login Timeout (minutes)..... 45
Baud Rate............................... 9600
Character Size.......................... 8
```

```
Flow Control:.............................. Disable
Stop Bits.................................. 1
Parity Type:............................... none
```

Related Topics

config serial baudrate
config serial timeout

config Commands

This section lists the **config** commands to configure controller ports and interfaces.

config interface address

To configure address information for an interface, use the **config interface address** command.

config interface address { **ap-manager** *IP_address netmask gateway* | **management** *IP_address netmask gateway* | **service-port** *IP_address netmask* | **virtual** *IP_address* | **dynamic-interface** *IP_address dynamic_interface netmask gateway* | **redundancy-management** *IP_address* **peer-redundancy-management** *IP_address* }

Syntax Description

ap-manager	Specifies the access point manager interface.
IP_address	IP address— IPv4 only.
netmask	Network mask.
gateway	IP address of the gateway.
management	Specifies the management interface.
service-port	Specifies the out-of-band service port interface.
virtual	Specifies the virtual gateway interface.
interface-name	Specifies the interface identified by the *interface-name* parameter.
interface-name	Interface name.
redundancy-management	Configures redundancy management interface IP address.
peer-redundancy-management	Configures the peer redundancy management interface IP address.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The management interface acts like an AP-manager interface by default.

This command is applicable for IPv4 addresses only.

Ensure that the management interfaces of both controllers are in the same subnet. Ensure that the Redundant Management IP address for both controllers is the same. Likewise, ensure that the Peer Redundant Management IP address for both the controllers is the same.

The following example shows how to configure an access point manager interface with IP address 209.165.201.31, network mask 255.255.0.0, and gateway address 209.165.201.30:

```
(Cisco Controller) > config interface address ap-manager 209.165.201.31 255.255.0.0
209.165.201.30
```

The following example shows how to configure a redundancy management interface on the controller:

```
(Cisco Controller) > config interface address redundancy-management 209.4.120.5
peer-redundancy-management 209.4.120.6
```

The following example shows how to configure a virtual interface:

```
(Cisco Controller) > config interface address virtual 192.0.2.1
```

Related Commands

show interface

Related Topics

show interface detailed, on page 256

config interface address

To configure interface addresses, use the **config interface address** command.

config interface address {**dynamic-interface** *dynamic_interface netmask gateway* | **management** | **redundancy-management** *IP_address* **peer-redundancy-management** | **service-port** *netmask* | **virtual**} *IP_address*

Syntax Description

dynamic-interface	Configures the dynamic interface of the controller.
dynamic_interface	Dynamic interface of the controller.
IP_address	IP address of the interface.
netmask	Netmask of the interface.
gateway	Gateway of the interface.
management	Configures the management interface IP address.
redundancy-management	Configures redundancy management interface IP address.
peer-redundancy-management	Configures the peer redundancy management interface IP address.
service-port	Configures the out-of-band service port.
virtual	Configures the virtual gateway interface.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Ensure that the management interfaces of both controllers are in the same subnet. Ensure that the redundant management IP address for both controllers is the same and that the peer redundant management IP address for both the controllers is the same.

The following example shows how to configure a redundancy management interface on the controller:

```
(Cisco Controller) >config interface address redundancy-management 209.4.120.5
peer-redundancy-management 209.4.120.6
```

The following example shows how to configure a virtual interface:

```
(Cisco Controller) > config interface address virtual 10.10.10.1
```

Related Commands

show interface group summary

show interface summary

config interface nasid

To configure the Network Access Server identifier (NAS-ID) for the interface, use the **config interface nasid** command.

config interface nasid {*NAS-ID* | **none**} *interface_name*

Syntax Description

NAS-ID	Network Access Server identifier (NAS-ID) for the interface. The NAS-ID is sent to the RADIUS server by the controller (as a RADIUS client) using the authentication request, which is used to classify users to different groups. You can enter up to 32 alphanumeric characters. Youcan configure the NAS-ID on the interface, WLAN, or an access point group. The order of priority is AP group NAS-ID > WLAN NAS-ID > Interface NAS-ID.
none	Configures the controller system name as the NAS-ID.
interface_name	Interface name up to 32 alphanumeric characters.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines The NAS-ID configured on the controller for AP group or WLAN or interface is used for authentication. The NAS-ID is not propagated across controllers.

The following example shows how to configure the NAS-ID for the interface:

```
(Cisco Controller) > config interface nasid
```

Related Commands

config wlan nasid

config wlan apgroup

config network profiling

To profile http port for a specific port, use the **config network profiling http-port** command.

config network profiling http-port *port number*

Syntax Description

port number	Interface port number. Default value is 80.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the http port in a network:

```
(Cisco Controller) > config network profiling http-port 80
```

config port adminmode

To enable or disable the administrative mode for a specific controller port or for all ports, use the **config port adminmode** command.

config port adminmode {**all** | *port*} {**enable** | **disable**}

Syntax Description

all	Configures all ports.
port	Number of the port.
enable	Enables the specified ports.
disable	Disables the specified ports.

Command Default Enabled

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to disable port 8:

```
(Cisco Controller) > config port adminmode 8 disable
```

The following example shows how to enable all ports:

```
(Cisco Controller) > config port adminmode all enable
```

Related Topics

config port autoneg
config port linktrap
config port multicast appliance
config port power
show port, on page 259

config route add

To configure a network route from the service port to a dedicated workstation IP address range, use the **config route add** command.

config route add *ip_address netmask gateway*

Syntax Description

ip_address	Network IP address.
netmask	Subnet mask for the network.
gateway	IP address of the gateway for the route network.

Command Default

None

Usage Guidelines

IP_address supports only IPv4 addresses.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure a network route to a dedicated workstation IP address 10.1.1.0, subnet mask 255.255.255.0, and gateway 10.1.1.1:

```
(Cisco Controller) > config route add 10.1.1.0 255.255.255.0 10.1.1.1
```

Related Topics

config route delete, on page 266

config route delete

To remove a network route from the service port, use the **config route delete** command.

config route delete *ip_address*

Syntax Description

ip_address	Network IP address.

Command Default

None

Usage Guidelines

IP_address supports only IPv4 addresses.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to delete a route from the network IP address 10.1.1.0:

```
(Cisco Controller) > config route delete 10.1.1.0
```

Related Topics

config route add, on page 266

VideoStream Commands

show Commands

This section lists the **show** commands to display information about your VideoStream configuration settings.

show 802.11

To display basic 802.11a, 802.11b/g, or 802.11h network settings, use the **show 802.11** command.

show 802.11{**a** | **b** | **h**}

Syntax Description

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

Command Default

None.

Command History

Release	Modification
8.3	This command was introduced.

This example shows to display basic 802.11a network settings:

```
> show 802.11a
802.11a Network.............................. Enabled
11nSupport................................... Enabled
      802.11a Low Band....................... Enabled
      802.11a Mid Band....................... Enabled
      802.11a High Band...................... Enabled
802.11a Operational Rates
    802.11a 6M Rate.......................... Mandatory
    802.11a 9M Rate.......................... Supported
    802.11a 12M Rate......................... Mandatory
    802.11a 18M Rate......................... Supported
    802.11a 24M Rate......................... Mandatory
    802.11a 36M Rate......................... Supported
    802.11a 48M Rate......................... Supported
    802.11a 54M Rate......................... Supported
802.11n MCS Settings:
    MCS 0.................................... Supported
    MCS 1.................................... Supported
    MCS 2.................................... Supported
    MCS 3.................................... Supported
    MCS 4.................................... Supported
    MCS 5.................................... Supported
    MCS 6.................................... Supported
    MCS 7.................................... Supported
    MCS 8.................................... Supported
    MCS 9.................................... Supported
    MCS 10................................... Supported
    MCS 11................................... Supported
    MCS 12................................... Supported
    MCS 13................................... Supported
```

```
    MCS 14..................................... Supported
    MCS 15..................................... Supported
802.11n Status:
    A-MPDU Tx:
        Priority 0..............................  Enabled
        Priority 1..............................  Disabled
        Priority 2..............................  Disabled
        Priority 3..............................  Disabled
        Priority 4..............................  Disabled
        Priority 5..............................  Disabled
        Priority 6..............................  Disabled
        Priority 7..............................  Disabled
Beacon Interval.................................  100
CF Pollable mandatory...........................  Disabled
CF Poll Request mandatory.......................  Disabled
--More-- or (q)uit
CFP Period......................................  4
CFP Maximum Duration............................  60
Default Channel.................................  36
Default Tx Power Level..........................  0
DTPC Status.....................................  Enabled
Fragmentation Threshold.........................  2346
TI Threshold....................................  -50
Legacy Tx Beamforming setting...................  Disabled
Traffic Stream Metrics Status...................  Enabled
Expedited BW Request Status.....................  Disabled
World Mode......................................  Enabled
EDCA profile type...............................  default-wmm
Voice MAC optimization status...................  Disabled
Call Admission Control (CAC) configuration
Voice AC:
   Voice AC - Admission control (ACM)...........  Disabled
   Voice max RF bandwidth.......................  75
   Voice reserved roaming bandwidth.............  6
   Voice load-based CAC mode....................  Disabled
   Voice tspec inactivity timeout...............  Disabled
   Voice Stream-Size............................  84000
   Voice Max-Streams............................  2
Video AC:
   Video AC - Admission control (ACM)...........  Disabled
   Video max RF bandwidth.......................  Infinite
   Video reserved roaming bandwidth.............  0
```

This example shows how to display basic 802.11h network settings:

```
> show 802.11h
802.11h ....................................... powerconstraint : 0
802.11h ....................................... channelswitch : Disable
802.11h ....................................... channelswitch mode : 0
```

Related Commands

show ap stats

show ap summary

show client summary

show network

show network summary

show port

show wlan

show 802.11 media-stream

To display the multicast-direct configuration state, use the **show 802.11 media-stream** command.

show 802.11 {**a** | **b** | **h**} **media-stream** *media_stream_name*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.
media_stream_name	Specified media stream name.

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 the media-stream configuration:

```
> show 802.11a media-stream rrc
Multicast-direct................................ Enabled
Best Effort..................................... Disabled
Video Re-Direct................................. Enabled
Max Allowed Streams Per Radio................... Auto
Max Allowed Streams Per Client.................. Auto
Max Video Bandwidth............................. 0
Max Voice Bandwidth............................. 75
Max Media Bandwidth............................. 85
Min PHY Rate.................................... 6000
Max Retry Percentage............................ 80
```

Related Commands **show media-stream group summary**

show media-stream client

To display the details for a specific media-stream client or a set of clients, use the **show media-stream client** command.

show media-stream client {*media-stream_name* | **summary**}

Syntax Description

media-stream_name	Name of the media-stream client of which the details is to be displayed.

summary	Displays the details for a set of media-stream clients.

Command Default None.

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to display a summary media-stream clients:

```
> show media-stream client summary
Number of Clients............................... 1
Client Mac         Stream Name  Stream Type  Radio WLAN  QoS    Status
-----------------  -----------  -----------  ----  ----  ------ -------
00:1a:73:dd:b1:12  mountainview  MC-direct    2.4   2     Video  Admitted
```

Related Commands **show media-stream group summary**

show media-stream group detail

To display the details for a specific media-stream group, use the **show media-stream group detail** command.

show media-stream group detail *media-stream_name*

Syntax Description

media-stream_name	Name of the media-stream group.

Command Default None.

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to display media-stream group configuration details:

```
> show media-stream group detail abc
Media Stream Name.............................. abc
Start IP Address............................... 227.8.8.8
End IP Address................................. 227.9.9.9
 RRC Parameters
 Avg Packet Size(Bytes)......................... 1200
 Expected Bandwidth(Kbps)....................... 300
 Policy......................................... Admit
 RRC re-evaluation.............................. periodic
 QoS............................................ Video
 Status......................................... Multicast-direct
 Usage Priority................................. 5
 Violation...................................... drop
```

Related Commands **show media-stream group summary**

show media-stream group summary

To display the summary of the media stream and client information, use the **show media-stream group summary** command.

show media-stream group summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to display a summary of the media-stream group:

```
(Cisco Controller) > show media-stream group summary
Stream Name   Start IP       End IP         Operation Status
------------- -------------- -------------- ----------------
abc           227.8.8.8      227.9.9.9      Multicast-direct
```

Related Commands

show 802.11 media-stream client

show media-stream client

show media-stream group detail

config Commands

This section lists the **config** commands to configure VideoStream settings on the controller.

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 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 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 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, on page 717
config advanced 802.11 channel update, on page 714

config 802.11 media-stream multicast-direct

To configure the media stream multicast-direct parameters for the 802.11 networks, use the **config 802.11 media-stream multicast-direct** command.

config 802.11 {**a** | **b**} **media-stream multicast-direct** {**admission-besteffort** {**enable** | **disable**} | {**client-maximum** | **radio-maximum**} {*value* | **no-limit** } | **enable** | **disable**}

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
admission-besteffort	Admits media stream to best-effort queue.
enable	Enables multicast-direct on a 2.4-GHz or a 5-GHz band.
disable	Disables multicast-direct on a 2.4-GHz or a 5-GHz band.
client-maximum	Specifies the maximum number of streams allowed on a client.
radio-maximum	Specifies the maximum number of streams allowed on a 2.4-GHz or a 5-GHz band.
value	Number of streams allowed on a client or on a 2.4-GHz or a 5-GHz band, between 1 to 20.
no-limit	Specifies the unlimited number of streams allowed on a client or on a 2.4-GHz or a 5-GHz band.

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.

Usage Guidelines

Before you configure the media stream multicast-direct parameters on a 802.11 network, ensure that the network is nonoperational.

This example shows how to enable a media stream multicast-direct settings on an 802.11a network:

```
> config 802.11a media-stream multicast-direct enable
```

This example shows how to admit the media stream to the best-effort queue:

```
> config 802.11a media-stream multicast-direct admission-besteffort enable
```

This example shows how to set the maximum number of streams allowed on a client:

```
> config 802.11a media-stream multicast-direct client-maximum 10
```

Related Commands

config 802.11 media-stream video-redirect

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config 802.11 media-stream video-redirect

To configure the media stream video-redirect for the 802.11 networks, use the **config 802.11 media-stream video-redirect** command.

config 802.11 {**a** | **b**} **media-stream video-redirect** {**enable** | **disable**}

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
enable	Enables traffic redirection.
disable	Disables traffic redirection.

Command Default

None.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Before you configure the media stream video-redirect on a 802.11 network, ensure that the network is nonoperational.

This example shows how to enable media stream traffic redirection on an 802.11a network:

```
> config 802.11a media-stream video-redirect enable
```

Related Commands

config 802.11 media-stream multicast-redirect

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream multicast-direct

To configure the media-stream multicast direct, use the **config media-stream multicast direct** command.

config media-stream multicast-direct {**enable** | **disable**}

Syntax Description

enable	Enables a media stream.
disable	Disables a media stream.

Command Default

None.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Media-stream multicast-direct requires load based Call Admission Control (CAC) to run.

This example shows how to enable media-stream multicast-direct settings:

```
> config media-stream multicast-direct enable
```

This example shows how to disable media-stream multicast-direct settings:

```
> config media-stream multicast-direct disable
```

Related Commands

config 802.11 media-stream video-redirect

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream message

To configure various parameters of message configuration, use the **config media-stream message** command.

config media-stream message {**state** [**enable** | **disable**] | **url** *url* | **email** *email* | **phone** *phone_number* | **note** *note*}

Syntax Description

state	Specifies the media stream message state.
enable	(Optional) Enables the session announcement message state.
disable	(Optional) Disables the session announcement message state.
url	Configures the URL.
url	Session announcement URL.
email	Configures the email ID.
email	Specifies the session announcement e-mail.

phone	Configures the phone number.
phone_number	Session announcement phone number.
note	Configures the notes.
note	Session announcement notes.

Command Default

Disabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Media-stream multicast-direct requires load-based Call Admission Control (CAC) to run.

This example shows how to enable the session announcement message state:

```
> config media-stream message state enable
```

This example shows how to configure the session announcement e-mail address:

```
> config media-stream message mail abc@co.com
```

Related Commands

config media-stream

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream add

To configure the various global media-stream configurations, use the **config media-stream add** command.

config media-stream add multicast-direct *media_stream_name start-IP end-IP* [**template** {**very coarse** | **coarse** | **ordinary** | **low-resolution** | **med-resolution** | **high-resolution**} | **detail** {*bandwidth packet-size* {**periodic** | **initial**}} **qos** *priority* {**drop** | **fallback**}

Syntax Description

multicast-direct	Specifies the media stream for the multicast-direct setting.
media_stream_name	Media-stream name.
start-IP	IP multicast destination start address.
end-IP	IP multicast destination end address.
template	(Optional) Configures the media stream from templates.
very coarse	Applies a very-coarse template.

coarse	Applies a coarse template.
ordinary	Applies an ordinary template.
low-resolution	Applies a low-resolution template.
med-resolution	Applies a medium-resolution template.
high-resolution	Applies a high-resolution template.
detail	Configures the media stream with specific parameters.
bandwidth	Maximum expected stream bandwidth.
packet-size	Average packet size.
periodic	Specifies the periodic admission evaluation.
initial	Specifies the Initial admission evaluation.
qos	AIR QoS class (video only).
priority	Media-stream priority.
drop	Specifies that the stream is dropped on a periodic reevaluation.
fallback	Specifies if the stream is demoted to the best-effort class on a periodic reevaluation.

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.

Usage Guidelines

Media-stream multicast-direct requires load-based Call Admission Control (CAC) to run.

This example shows how to configure a new media stream:

```
> config media-stream add multicast-direct abc 227.8.8.8 227.9.9.9 detail 2 150 periodic
video 1 drop
```

Related Commands

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream admit

To allow traffic for a media stream group, use the **config media-stream admit** command.

config media-stream admit *media_stream_name*

Syntax Description

media_stream_name	Media-stream group name.

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.

Usage Guidelines

When you try to allow traffic for the media stream group, you will be prompted that IGMP snooping will be disabled and enabled again, and all clients might observe a glitch on the multicast traffic.

This example shows how to allow traffic for a media stream group:

```
(Cisco Controller) > config media-stream admit MymediaStream
```

Related Commands

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream deny

To block traffic for a media stream group, use the **config media-stream deny** command.

Syntax Description

media_stream_name	Media-stream group name.

config media-stream deny *media_stream_name*

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.

Usage Guidelines

When you try to block traffic for the media stream group, you will be prompted that IGMP snooping will be disabled and enabled again, and all clients might observe a glitch on the multicast traffic.

This example shows how to block traffic for a media stream group:

```
(Cisco Controller) > config media-stream deny MymediaStream
```

Related Commands

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream delete

To configure the various global media-stream configurations, use the **config media-stream delete** command.

config media-stream delete *media_stream_name*

Syntax Description

media_stream_name	Media-stream name.

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.

Usage Guidelines

Media-stream multicast-direct requires load-based Call Admission Control (CAC) to run.

This example shows how to delete the media stream named abc:

```
(Cisco Controller) > config media-stream delete abc
```

Related Commands

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config wlan media-stream

To configure multicast-direct for a wireless LAN media stream, use the **config wlan media-stream** command.

config wlan media-stream multicast-direct {*wlan_id* | **all**} {**enable** | **disable**}

Syntax Description

multicast-direct	Configures multicast-direct for a wireless LAN media stream.
wlan_id	Wireless LAN identifier between 1 and 512.
all	Configures the wireless LAN on all media streams.
enable	Enables global multicast to unicast conversion.
disable	Disables global multicast to unicast conversion.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Media stream multicast-direct requires load based Call Admission Control (CAC) to run. WLAN quality of service (QoS) needs to be set to either gold or platinum.

The following example shows how to enable the global multicast-direct media stream with WLAN ID 2:

```
(Cisco Controller) >config wlan media-stream multicast-direct 2 enable
```

Security Commands

show Commands

This section lists the **show** commands to display information about your security configuration settings for the controller.

show 802.11

To display basic 802.11a, 802.11b/g, or 802.11h network settings, use the **show 802.11** command.

show 802.11 {**a** | **b** | **h**}

Syntax Description

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

Command Default

None.

Command History

Release	Modification
8.3	This command was introduced.

This example shows to display basic 802.11a network settings:

```
>  show 802.11a
802.11a Network.............................. Enabled
11nSupport................................... Enabled
      802.11a Low Band....................... Enabled
      802.11a Mid Band....................... Enabled
      802.11a High Band...................... Enabled
802.11a Operational Rates
    802.11a 6M Rate.......................... Mandatory
    802.11a 9M Rate.......................... Supported
    802.11a 12M Rate......................... Mandatory
    802.11a 18M Rate......................... Supported
    802.11a 24M Rate......................... Mandatory
    802.11a 36M Rate......................... Supported
    802.11a 48M Rate......................... Supported
    802.11a 54M Rate......................... Supported
802.11n MCS Settings:
    MCS 0.................................... Supported
    MCS 1.................................... Supported
    MCS 2.................................... Supported
    MCS 3.................................... Supported
    MCS 4.................................... Supported
    MCS 5.................................... Supported
    MCS 6.................................... Supported
    MCS 7.................................... Supported
    MCS 8.................................... Supported
    MCS 9.................................... Supported
    MCS 10................................... Supported
    MCS 11................................... Supported
    MCS 12................................... Supported
```

```
    MCS 13..................................... Supported
    MCS 14..................................... Supported
    MCS 15..................................... Supported
802.11n Status:
    A-MPDU Tx:
        Priority 0............................. Enabled
        Priority 1............................. Disabled
        Priority 2............................. Disabled
        Priority 3............................. Disabled
        Priority 4............................. Disabled
        Priority 5............................. Disabled
        Priority 6............................. Disabled
        Priority 7............................. Disabled
Beacon Interval................................ 100
CF Pollable mandatory.......................... Disabled
CF Poll Request mandatory...................... Disabled
--More-- or (q)uit
CFP Period..................................... 4
CFP Maximum Duration........................... 60
Default Channel................................ 36
Default Tx Power Level......................... 0
DTPC Status.................................... Enabled
Fragmentation Threshold........................ 2346
TI Threshold................................... -50
Legacy Tx Beamforming setting.................. Disabled
Traffic Stream Metrics Status.................. Enabled
Expedited BW Request Status.................... Disabled
World Mode..................................... Enabled
EDCA profile type.............................. default-wmm
Voice MAC optimization status.................. Disabled
Call Admission Control (CAC) configuration
Voice AC:
   Voice AC - Admission control (ACM)..... Disabled
   Voice max RF bandwidth................. 75
   Voice reserved roaming bandwidth....... 6
   Voice load-based CAC mode.............. Disabled
   Voice tspec inactivity timeout......... Disabled
   Voice Stream-Size...................... 84000
   Voice Max-Streams...................... 2
Video AC:
   Video AC - Admission control (ACM)..... Disabled
   Video max RF bandwidth................. Infinite
   Video reserved roaming bandwidth....... 0
```

This example shows how to display basic 802.11h network settings:

```
> show 802.11h
802.11h ....................................... powerconstraint : 0
802.11h ....................................... channelswitch : Disable
802.11h ....................................... channelswitch mode : 0
```

Related Commands

show ap stats

show ap summary

show client summary

show network

show network summary

show port

show wlan

show aaa auth

To display the configuration settings for the AAA authentication server database, use the **show aaa auth** command.

show aaa 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 display the configuration settings for the AAA authentication server database:

```
(Cisco Controller) > show aaa auth
Management authentication server order:
    1..................................... local
    2..................................... tacacs
```

Related Commands **config aaa auth**

config aaa auth mgmt

show advanced eap

To display Extensible Authentication Protocol (EAP) settings, use the **show advanced eap** command.

show advanced eap

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 EAP settings:

```
(Cisco Controller) > show advanced eap
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries.......... 20
EAP Key-Index for Dynamic WEP............. 0
```

```
EAP Max-Login Ignore Identity Response.......... enable
EAP-Request Timeout (seconds)................... 1
EAP-Request Max Retries......................... 20
EAPOL-Key Timeout (milliseconds)................ 1000
EAPOL-Key Max Retries........................... 2
```

Related Commands

config advanced eap

config advanced timers eap-identity-request-delay

config advanced timers eap-timeout

show client detail

To display IP addresses per client learned through DNS snooping (DNS-based ACL), use the **show client detail** *mac_address* command.

show client detail *mac_address*

Syntax Description

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 client detail** *mac_address* command.

```
(Cisco Controller) > show client detail 01:35:6x:yy:21:00
 Client MAC Address.............................. 01:35:6x:yy:21:00
Client Username ................................. test
AP MAC Address.................................. 00:11:22:33:44:x0
AP Name......................................... AP0011.2020.x111
AP radio slot Id................................ 1
Client State.................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id................................. 7
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 00:11:22:33:44:xx
Connected For .................................. 28 secs
Channel......................................... 56
IP Address...................................... 10.0.0.1
Gateway Address................................. Unknown
Netmask......................................... Unknown
IPv6 Address.................................... xx20::222:6xyy:zeeb:2233
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 1
Status Code..................................... 0
Client CCX version.............................. No CCX support
```

```
Re-Authentication Timeout..................... 1756
QoS Level..................................... Silver
Avg data Rate................................. 0
Burst data Rate............................... 0
Avg Real time data Rate....................... 0
Burst Real Time data Rate..................... 0
802.1P Priority Tag........................... disabled
CTS Security Group Tag........................ Not Applicable
KTS CAC Capability............................ No
WMM Support................................... Enabled
  APSD ACs.....................................  BK  BE  VI  VO
Power Save.................................... ON
Current Rate.................................. m7
Supported Rates..............................
6.0,9.0,12.0,18.0,24.0,36.0,
    ..................................... 48.0,54.0
Mobility State................................ Local
Mobility Move Count........................... 0
Security Policy Completed..................... No
Policy Manager State..........................SUPPLICANT_PROVISIONING
Policy Manager Rule Created................... Yes
AAA Override ACL Name......................... android
AAA Override ACL Applied Status............... Yes
AAA Override Flex ACL Name.................... none
AAA Override Flex ACL Applied Status.......... Unavailable
AAA URL redirect.............................
https://10.0.0.3:8443/guestportal/gateway?sessionId=0a68aa72000000015272404e&action=nsp
Audit Session ID.............................. 0a68aa72000000015272404e
AAA Role Type................................. none
Local Policy Applied.......................... p1
IPv4 ACL Name................................. none
FlexConnect ACL Applied Status................ Unavailable
IPv4 ACL Applied Status....................... Unavailable
IPv6 ACL Name................................. none
IPv6 ACL Applied Status....................... Unavailable
Layer2 ACL Name............................... none
Layer2 ACL Applied Status..................... Unavailable
Client Type................................... SimpleIP
mDNS Status................................... Enabled
mDNS Profile Name............................. default-mdns-profile
No. of mDNS Services Advertised............... 0
Policy Type................................... WPA2
Authentication Key Management................. 802.1x
Encryption Cipher............................. CCMP (AES)
Protected Management Frame ................... No
Management Frame Protection................... No
EAP Type...................................... PEAP
Interface..................................
.. management
VLAN.......................................... 0
Quarantine VLAN............................... 0
```

```
Access VLAN..................................... 0
Client Capabilities:
      CF Pollable............................... Not implemented
      CF Poll Request........................... Not implemented
      Short Preamble............................ Not implemented
      PBCC...................................... Not implemented
      Channel Agility........................... Not implemented
      Listen Interval........................... 10
      Fast BSS Transition....................... Not implemented
Client Wifi Direct Capabilities:
      WFD capable............................... No
      Manged WFD capable........................ No
      Cross Connection Capable.................. No
      Support Concurrent Operation.............. No
Fast BSS Transition Details:
Client Statistics:
      Number of Bytes Received.................. 123659
      Number of Bytes Sent...................... 120564
      Number of Packets Received................ 1375
      Number of Packets Sent.................... 276
      Number of Interim-Update Sent............. 0
      Number of EAP Id Request Msg Timeouts..... 0
      Number of EAP Id Request Msg Failures..... 0
      Number of EAP Request Msg Timeouts........ 2
      Number of EAP Request Msg Failures........ 0
      Number of EAP Key Msg Timeouts............ 0
      Number of EAP Key Msg Failures............ 0
      Number of Data Retries.................... 82
      Number of RTS Retries..................... 0
      Number of Duplicate Received Packets...... 0
      Number of Decrypt Failed Packets.......... 0
      Number of Mic Failured Packets............ 0
      Number of Mic Missing Packets............. 0
      Number of RA Packets Dropped.............. 0
      Number of Policy Errors................... 0
      Radio Signal Strength Indicator........... -51 dBm
      Signal to Noise Ratio..................... 46 dB
Client Rate Limiting Statistics:
      Number of Data Packets Recieved........... 0
      Number of Data Rx Packets Dropped......... 0
      Number of Data Bytes Recieved............. 0
      Number of Data Rx Bytes Dropped........... 0
      Number of Realtime Packets Recieved....... 0
      Number of Realtime Rx Packets Dropped..... 0
      Number of Realtime Bytes Recieved......... 0
      Number of Realtime Rx Bytes Dropped....... 0
      Number of Data Packets Sent............... 0
      Number of Data Tx Packets Dropped......... 0
      Number of Data Bytes Sent................. 0
      Number of Data Tx Bytes Dropped........... 0
      Number of Realtime Packets Sent........... 0
```

```
      Number of Realtime Tx Packets Dropped...... 0
      Number of Realtime Bytes Sent.............. 0
      Number of Realtime Tx Bytes Dropped........ 0
Nearby AP Statistics:
      AP0022.9090.c545(slot 0)
        antenna0: 26 secs ago..................... -33 dBm
        antenna1: 26 secs ago..................... -35 dBm
      AP0022.9090.c545(slot 1)
        antenna0: 25 secs ago..................... -41 dBm
        antenna1: 25 secs ago..................... -44 dBm
      APc47d.4f3a.35c2(slot 0)
        antenna0: 26 secs ago..................... -30 dBm
        antenna1: 26 secs ago..................... -36 dBm
      APc47d.4f3a.35c2(slot 1)
        antenna0: 24 secs ago..................... -43 dBm
        antenna1: 24 secs ago..................... -45 dBm
DNS Server details:
      DNS server IP ............................. 0.0.0.0
      DNS server IP ............................. 0.0.0.0

Client Dhcp Required:     False
Allowed (URL)IP Addresses
-------------------------
209.165.200.225
209.165.200.226
209.165.200.227
209.165.200.228
209.165.200.229
209.165.200.230
209.165.200.231
209.165.200.232
209.165.200.233
209.165.200.234
209.165.200.235
209.165.200.236
209.165.200.237
209.165.200.238
209.165.201.1
209.165.201.2
209.165.201.3
209.165.201.4
209.165.201.5
209.165.201.6
209.165.201.7
209.165.201.8
209.165.201.9
209.165.201.10
```

Related Topics

config acl url-domain

show acl detailed

show acl summary

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 exclusionlist

To display a summary of all clients on the manual exclusion list from associating with the controller, use the **show exclusionlist** command.

show exclusionlist

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines This command displays all manually excluded MAC addresses.

The following example shows how to display the exclusion list:

```
(Cisco Controller) > show exclusionlist
No manually disabled clients.
Dynamically Disabled Clients
----------------------------
  MAC Address             Exclusion Reason        Time Remaining (in secs)
  -----------             ----------------        ------------------------
00:40:96:b4:82:55         802.1X Failure           51
```

Related Commands **config exclusionlist**

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 local-auth config

To display local authentication configuration information, use the **show local-auth config** command.

show local-auth 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 display the local authentication configuration information:

```
(Cisco Controller) > show local-auth config
User credentials database search order:
Primary ..................................... Local DB
Configured EAP profiles:
Name ........................................ fast-test
Certificate issuer ..................... default
Enabled methods ........................ fast
Configured on WLANs ................... 2
EAP Method configuration:
EAP-TLS:
Certificate issuer ..................... default
Peer verification options:
 Check against CA certificates ..... Enabled
 Verify certificate CN identity .... Disabled
 Check certificate date validity ... Enabled
EAP-FAST:
TTL for the PAC ........................ 3 600
Initial client message ................. <none>
Local certificate required ............. No
Client certificate required ........... No
Vendor certificate required ........... No
Anonymous provision allowed ........... Yes
Authenticator ID ....................... 7b7fffffff0000000000000000000000
Authority Information .................. Test
EAP Profile..................................... tls-prof
Enabled methods for this profile .......... tls
Active on WLANs ........................... 1 3EAP Method configuration:
EAP-TLS:
Certificate issuer used ............... cisco
Peer verification options:
 Check against CA certificates ..... disabled
 Verify certificate CN identity .... disabled
 Check certificate date validity ... disabled
```

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 certificates

show local-auth statistics

show local-auth statistics

To display local Extensible Authentication Protocol (EAP) authentication statistics, use the **show local-auth statistics** command:

show local-auth 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 display the local authentication certificate statistics:

```
(Cisco Controller) > show local-auth statistics
Local EAP authentication DB statistics:
Requests received ..............................  14
Responses returned .............................  14
Requests dropped (no EAP AVP) ..................  0
Requests dropped (other reasons) ...............  0
Authentication timeouts ........................  0
Authentication statistics:
  Method          Success         Fail
  ------------------------------------
  Unknown               0            0
  LEAP                  0            0
  EAP-FAST              2               0
  EAP-TLS               0            0
  PEAP                  0            0
Local EAP credential request statistics:
Requests sent to LDAP DB .......................  0
Requests sent to File DB .......................  2
Requests failed (unable to send) ...............  0
Authentication results received:
  Success ......................................  2
  Fail .........................................  0
Certificate operations:
Local device certificate load failures ..........  0
Total peer certificates checked ................  0
Failures:
  CA issuer check ..............................  0
  CN name not equal to identity ................  0
  Dates not valid or expired ...................  0
```

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 certificates

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 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 radius acct detailed

To display RADIUS accounting server information, use the **show radius acct detailed** command.

show radius acct detailed *radius_index*

Syntax Description

radius_index	Radius server index. The range is from 1 to 17.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display RADIUS accounting server information:

```
(Cisco Controller) > show radius acct detailed 5

Radius Index........5
NAI Realms..........LAB.VTV.BLR.cisco.co.in
```

show radius acct statistics

To display the RADIUS accounting server statistics for the Cisco wireless LAN controller, use the **show radius acct statistics** command.

show radius acct 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 display RADIUS accounting server statistics:

```
(Cisco Controller) > show radius acct statistics
Accounting Servers:
Server Index..................................... 1
Server Address................................... 10.1.17.10
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 0
Retry Requests................................... 0
Accounting Responses............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Related Commands

config radius acct

config radius acct ipsec authentication

config radius acct ipsec disable

config radius acct network

show radius auth statistics

show radius summary

show radius auth detailed

To display RADIUS authentication server information, use the **show radius auth detailed** command.

show radius auth detailed *radius_index*

Syntax Description

radius_index	Radius server index. The range is from 1 to 17.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display RADIUS authentication server information:

```
(Cisco Controller) > show radius auth detailed 1

Radius Index........1
NAI Realms..........LAB.VTV.BLR.cisco.co.in
```

show radius auth statistics

To display the RADIUS authentication server statistics for the Cisco wireless LAN controller, use the **show radius auth statistics** command.

show radius auth statistics

This command has no arguments or keyword.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display RADIUS authentication server statistics:

```
(Cisco Controller) > show radius auth statistics
Authentication Servers:
  Server Index..................................... 1
  Server Address................................... 209.165.200.10
  Msg Round Trip Time.............................. 0 (1/100 second)
  First Requests................................... 0
  Retry Requests................................... 0
  Accept Responses................................. 0
  Reject Responses................................. 0
  Challenge Responses.............................. 0
  Malformed Msgs................................... 0
  Bad Authenticator Msgs........................... 0
  Pending Requests................................. 0
  Timeout Requests................................. 0
  Unknowntype Msgs................................. 0
  Other Drops...................................... 0
```

Related Commands

config radius auth

config radius auth management

config radius auth network

show radius summary

show radius avp-list

To display RADIUS VSA AVPs, use the **show radius avp-list** command.

show radius avp-list *profile-name*

Syntax Description

profile-name	Profile name for which downloaded AVPs to be shown.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display RADIUS VSA AVPs:

```
(Cisco Controller) > show radius avp-list
```

show radius summary

To display the RADIUS authentication and accounting server summary, use the **show radius summary** command.

show radius summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a RADIUS authentication server summary:

```
(Cisco Controller) > show radius summary
Vendor Id Backward Compatibility..................... Disabled
Credentials Caching.................................. Disabled
Call Station Id Type................................. IP Address
Administrative Authentication via RADIUS......... Enabled
Authentication Servers
Index  Type  Server Address    Port    State     Tout  RFC-3576  IPsec -
 AuthMod
e/Phase1/Group/Lifetime/Auth/Encr
-----  ----  ---------------  ------  --------  ----  --------  ---------------
--------------------------------
```

```
Accounting Servers
Index  Type  Server Address    Port    State     Tout  RFC-3576  IPsec -
 AuthMod
e/Phase1/Group/Lifetime/Auth/Encr
-----  ----  ---------------  ------  --------  ----  --------  ---------------
--------------------------------
```

Related Commands

show radius auth statistics

show radius acct statistics

show rules

To display the active internal firewall rules, use the **show rules** command.

show rules

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 active internal firewall rules:

```
(Cisco Controller) > show rules
-------------------------------------------------------
Rule ID.............: 3
Ref count...........: 0
Precedence..........: 99999999
Flags...............: 00000001 ( PASS )
Source IP range:
        (Local stack)
Destination IP range:
        (Local stack)
-------------------------------------------------------
Rule ID.............: 25
Ref count...........: 0
Precedence..........: 99999999
Flags...............: 00000001 ( PASS )
Service Info
        Service name........: GDB
        Protocol............: 6
        Source port low.....: 0
        Source port high....: 0
        Dest port low.......: 1000
        Dest port high......: 1000
Source IP range:
```

```
IP High.............: 0.0.0.0
        Interface..........: ANY
Destination IP range:
        (Local stack)
-------------------------------------------------------
```

show rogue adhoc custom summary

To display information about custom rogue ad-hoc rogue access points, use the **show rogue adhoc custom summary** command.

show rogue adhoc custom summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display details of custom rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc custom summary
Number of Adhocs............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

Related Commands

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc friendly summary

show rogue adhoc malicious summary

show rogue adhoc unclassified summary

config rogue adhoc

show rogue adhoc detailed

To display details of an ad-hoc rogue access point detected by the Cisco wireless LAN controller, use the **show rogue adhoc client detailed** command.

show rogue adhoc detailed *MAC_address*

Syntax Description

MAC_address	Adhoc rogue MAC address.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display detailed ad-hoc rogue MAC address information:

```
(Cisco Controller) > show rogue adhoc client detailed 02:61:ce:8e:a8:8c
Adhoc Rogue MAC address..................... 02:61:ce:8e:a8:8c
Adhoc Rogue BSSID........................... 02:61:ce:8e:a8:8c
State....................................... Alert
First Time Adhoc Rogue was Reported.............. Tue Dec 11 20:45:45
2007
Last Time Adhoc Rogue was Reported.............. Tue Dec 11 20:45:45
2007
Reported By
AP 1
MAC Address............................. 00:14:1b:58:4a:e0
Name.................................... AP0014.1ced.2a60
Radio Type.............................. 802.11b
SSID.................................... rf4k3ap
Channel................................. 3
RSSI.................................... -56 dBm
SNR..................................... 15 dB
Encryption.............................. Disabled
ShortPreamble........................... Disabled
WPA Support............................. Disabled
Last reported by this AP.............. Tue Dec 11 20:45:45 2007
```

Related Commands

config rogue adhoc

show rogue ignore-list

show rogue rule summary

show rogue rule detailed

config rogue rule

show rogue adhoc summary

show rogue adhoc friendly summary

To display information about friendly rogue ad-hoc rogue access points, use the **show rogue adhoc friendly summary** command.

show rogue adhoc friendly summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display information about friendly rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc friendly summary

Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

Related Commands

show rogue adhoc custom summary

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc malicious summary

show rogue adhoc unclassified summary

config rogue adhoc

show rogue adhoc malicious summary

To display information about malicious rogue ad-hoc rogue access points, use the **show rogue adhoc malicious summary** command.

show rogue adhoc malicious summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display details of malicious rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc malicious summary
Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

Related Commands

show rogue adhoc custom summary

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc friendly summary

show rogue adhoc unclassified summary

config rogue adhoc

show rogue adhoc unclassified summary

To display information about unclassified rogue ad-hoc rogue access points, use the **show rogue adhoc unclassified summary** command.

show rogue adhoc unclassified summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display information about unclassified rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc unclassified summary

Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

Related Commands

show rogue adhoc custom summary

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc friendly summary

show rogue adhoc malicious summary

config rogue adhoc

show rogue adhoc summary

To display a summary of the ad-hoc rogue access points detected by the Cisco wireless LAN controller, use the **show rogue adhoc summary** command.

show rogue adhoc summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a summary of all ad-hoc rogues:

```
(Cisco Controller) > show rogue adhoc summary
Detect and report Ad-Hoc Networks..... Enabled
Client MAC Address   Adhoc BSSID    State  # APs       Last Heard
------------------   -----------    -----   ---       -------
xx:xx:xx:xx:xx:xx    super          Alert    1         Sat Aug  9 21:12:50
 2004
xx:xx:xx:xx:xx:xx                    Alert    1          Aug  9 21:12:50
2003
xx:xx:xx:xx:xx:xx                   Alert    1         Sat Aug  9 21:10:50
 2003
```

Related Commands

config rogue adhoc

show rogue ignore-list

show rogue rule summary

show rogue rule detailed

config rogue rule

show rogue adhoc detailed

show rogue ap custom summary

To display information about custom rogue ad-hoc rogue access points, use the **show rogue ap custom summary** command.

show rogue ap custom summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display details of custom rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue ap custom summary

Number of APs.............................0

MAC Address        State              # APs # Clients Last Heard
```

```
----------------   ------------------ -----  ---------
-----------------------
```

Related Commands

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap clients

To display details of rogue access point clients detected by the Cisco wireless LAN controller, use the **show rogue ap clients** command.

show rogue ap clients *ap_mac_address*

Syntax Description

ap_mac_address	Rogue access point MAC address.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display details of rogue access point clients:

```
(Cisco Controller) > show rogue ap clients xx:xx:xx:xx:xx:xx
```

```
MAC Address State # APs Last Heard
----------------- ------------------ ----- -------------------------
00:bb:cd:12:ab:ff Alert 1 Fri Nov 30 11:26:23 2007
```

Related Commands

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

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 client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap detailed

To display details of a rogue access point detected by the Cisco wireless LAN controller, use the **show rogue-ap detailed** command.

show rogue ap detailed *ap_mac_address*

Syntax Description

ap_mac_address	Rogue access point MAC address.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display detailed information of a rogue access point:

```
(Cisco Controller) > show rogue ap detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..................................... 00:0b:85:63:d1:94
Is Rogue on Wired Network....................... No
Classification.................................. Unclassified
State........................................... Alert
First Time Rogue was Reported................... Fri Nov 30 11:24:56
2007
Last Time Rogue was Reported.................... Fri Nov 30 11:24:56
2007
Reported By
AP 1
MAC Address.............................. 00:12:44:bb:25:d0
Name..................................... flexconnect
Radio Type............................... 802.11g
SSID..................................... edu-eap
Channel.................................. 6
RSSI..................................... -61 dBm
SNR...................................... -1 dB
Encryption............................... Enabled
ShortPreamble............................ Enabled
WPA Support.............................. Disabled
Last reported by this AP.............. Fri Nov 30 11:24:56 2007
```

This example shows how to display detailed information of a rogue access point with a customized classification:

```
(Cisco Controller) > show rogue ap detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..................................... 00:17:0f:34:48:a0
Is Rogue on Wired Network....................... No
Classification.................................. custom
Severity Score ................................. 1
Class Name.....................................VeryMalicious
Class Change by................................. Rogue Rule
Classified at .................................. -60 dBm
Classified by................................... c4:0a:cb:a1:18:80

State........................................... Contained
State change by................................. Rogue Rule
First Time Rogue was Reported................... Mon Jun  4 10:31:18
2012
Last Time Rogue was Reported.................... Mon Jun  4 10:31:18
2012
Reported By
    AP 1
        MAC Address.............................. c4:0a:cb:a1:18:80
        Name..................................... SHIELD-3600-2027
        Radio Type............................... 802.11g
        SSID..................................... sri
        Channel.................................. 11
        RSSI..................................... -87 dBm
```

```
        SNR..................................... 4 dB
        Encryption.............................. Enabled
        ShortPreamble........................... Enabled
        WPA Support............................. Enabled
        Last reported by this AP................ Mon Jun  4 10:31:18
2012
```

Related Commands

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap summary

To display a summary of the rogue access points detected by the Cisco wireless LAN controller, use the **show rogue-ap summary** command.

show rogue ap summary{**ssid** | **channel**}

Syntax Description

ssid	Displays specific user-configured SSID of the rogue access point.
channel	Displays specific user-configured radio type and channel of the rogue access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a summary of all rogue access points:

```
(Cisco Controller) > show rogue ap summary

Rogue Location Discovery Protocol.................  Disabled
Rogue ap timeout..............................  1200
Rogue on wire Auto-Contain..................... Disabled
Rogue using our SSID Auto-Contain.............. Disabled
Valid client on rogue AP Auto-Contain.......... Disabled
Rogue AP timeout............................... 1200
Rogue Detection Report Interval................ 10
Rogue Detection Min Rssi....................... -128
Rogue Detection Transient Interval............. 0
Rogue Detection Client Num Thershold............ 0
Total Rogues(AP+Ad-hoc) supported.............. 2000
Total Rogues classified........................ 729

MAC Address        Classification     # APs # Clients Last Heard
-----------------  ------------------ ----- --------- -----------------------
xx:xx:xx:xx:xx:xx  friendly           1     0         Thu Aug  4 18:57:11 2005
xx:xx:xx:xx:xx:xx  malicious          1     0         Thu Aug  4 19:00:11 2005
xx:xx:xx:xx:xx:xx  malicious          1     0         Thu Aug  4 18:57:11 2005
xx:xx:xx:xx:xx:xx  malicious          1     0         Thu Aug  4 18:57:11 2005
```

The following example shows how to display a summary of all rogue access points with SSID as extended parameter.

```
(Cisco Controller) > show rogue ap summary ssid

MAC Address        Class              State      SSID  Security
-------------------------------------------------------------------------------------

xx:xx:xx:xx:xx:xx  Unclassified       Alert       xxx   Open
xx:xx:xx:xx:xx:xx  Unclassified       Alert       xxx   Open
xx:xx:xx:xx:xx:xx  Pending            Pending     xxx   Open
xx:xx:xx:xx:xx:xx  Unclassified       Alert       xxx   WEP/WPA
```

The following example shows how to display a summary of all rogue access points with channel as extended parameter.

```
(Cisco Controller) > show rogue ap summary channel

MAC Address        Class              State  Det RadioType    Channel RSSIlast/Max)
-------------------------------------------------------------------------------------------------

xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11g           11    -53 / -48
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11g           11    -53 / -48
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11a           149    -74 / -69
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11a           149    -74 / -69
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11a           149    -74 / -69
```

The following example shows how to display a summary of all rogue access points with both SSID and channel as extended parameters.

```
(Cisco Controller) > show rogue ap summary ssid channel

MAC Address        Class        State    SSID                  Security  Det RadioType
Channel  RSSI(last/Max)
-------------------------------------------------------------------------------------------------
```

```
xx:xx:xx:xx:xx:xx  Unclassified  Alert   dd                  WEP/WPA     802.11n5G
56    -73 / -62
xx:xx:xx:xx:xx:xx  Unclassified  Alert   SSID IS HIDDEN      Open        802.11a
149   -68 / -66
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan16              WEP/WPA     802.11n5G
149   -71 / -71
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan15              WEP/WPA     802.11n5G
149   -71 / -71
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan14              WEP/WPA     802.11n5G
149   -71 / -71
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan13              WEP/WPA     802.11n5G
149   -71 / -70
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan12              WEP/WPA     802.11n5G
149   -71 / -71
```

Related Commands

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap friendly summary

To display a list of the friendly rogue access points detected by the controller, use the **show rogue ap friendly summary** command.

show rogue ap friendly summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a summary of all friendly rogue access points:

```
(Cisco Controller) > show rogue ap friendly summary
Number of APs.................................... 1
MAC Address       State     # APs  # Clients Last Heard
----------------- ------------------ ----- ---------
--------------------------
XX:XX:XX:XX:XX:XX Internal    1    0  Tue Nov 27 13:52:04 2007
```

Related Commands

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap malicious summary

To display a list of the malicious rogue access points detected by the controller, use the **show rogue ap malicious summary** command.

show rogue ap malicious summary

Syntax Description

This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a summary of all malicious rogue access points:

```
(Cisco Controller) > show rogue ap malicious summary
Number of APs.................................... 2
MAC Address       State     # APs  # Clients Last Heard
----------------- ------------------ ----- ---------
--------------------------
XX:XX:XX:XX:XX:XX Alert           1   0  Tue Nov 27 13:52:04 2007
XX:XX:XX:XX:XX:XX Alert           1   0  Tue Nov 27 13:52:04 2007
```

Related Commands

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap unclassified summary

To display a list of the unclassified rogue access points detected by the controller, use the **show rogue ap unclassified summary** command.

show rogue ap unclassified summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a list of all unclassified rogue access points:

```
(Cisco Controller) > show rogue ap unclassified summary
Number of APs.................................. 164
MAC Address      State  # APs # Clients Last Heard
---------------- ------------- ----- --------- ---------------
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:12:52 2007
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:29:01 2007
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:26:23 2007
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:26:23 2007
```

show rogue client detailed

To display details of a rogue client detected by a Cisco wireless LAN controller, use the **show rogue client detailed** command.

show rogue client detailed *Rogue_AP MAC_address*

Syntax Description

Rogue_AP	Rogue AP address.
MAC_address	Rogue client MAC address.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display detailed information for a rogue client:

```
(Cisco Controller) > show rogue client detailed xx:xx:xx:xx:xx:xx
Rogue BSSID.................................... 00:0b:85:23:ea:d1
State.......................................... Alert
First Time Rogue was Reported.................. Mon Dec 3 21:50:36 2007
Last Time Rogue was Reported................... Mon Dec 3 21:50:36 2007
Rogue Client IP address........................ Not known
Reported By
AP 1
MAC Address.............................. 00:15:c7:82:b6:b0
Name..................................... AP0016.47b2.31ea
Radio Type............................... 802.11a
RSSI..................................... -71 dBm
SNR...................................... 23 dB
```

```
Channel.................................. 149
Last reported by this AP.............. Mon Dec 3 21:50:36 2007
```

Related Commands

show rogue client summary

show rogue ignore-list

config rogue rule client

config rogue rule

show rogue client summary

To display a summary of the rogue clients detected by the Cisco wireless LAN controller, use the **show rogue client summary** command.

show rogue client summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a list of all rogue clients:

```
(Cisco Controller) > show rogue client summary
Validate rogue clients against AAA.............. Disabled
Total Rogue Clients supported.................... 2500
Total Rogue Clients present...................... 3
MAC Address        State              # APs Last Heard
-----------------  -----------------  ----- ----------------------
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:09:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:03:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:03:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:09:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 18:57:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:12:08 2005
```

Related Commands

show rogue client detailed

show rogue ignore-list

config rogue client

config rogue rule

show rogue ignore-list

To display a list of rogue access points that are configured to be ignored, use the **show rogue ignore-list** command.

show rogue ignore-list

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a list of all rogue access points that are configured to be ignored.

```
(Cisco Controller) > show rogue ignore-list

MAC Address
-----------------
xx:xx:xx:xx:xx:xx
```

Related Commands

config rogue adhoc

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

config rogue rule

config trapflags rogueap

show rogue client detailed

show rogue ignore-list

show rogue rule summary

show rogue client summary

show rogue ap unclassified summary

show rogue ap malicious summary

show rogue ap friendly summary

config rogue client

show rogue ap summary

show rogue ap clients

show rogue ap detailed

config rogue rule

show rogue rule detailed

To display detailed information for a specific rogue classification rule, use the **show rogue rule detailed** command.

show rogue rule detailed *rule_name*

Syntax Description

rule_name	Rogue rule name.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display detailed information on a specific rogue classification rule:

```
(Cisco Controller) > show rogue rule detailed Rule2
Priority..................................... 2
Rule Name.................................... Rule2
State........................................ Enabled
Type......................................... Malicious
Severity Score............................... 1
Class Name................................... Very_Malicious
Notify....................................... All
State ....................................... Contain
Match Operation.............................. Any
Hit Count.................................... 352
Total Conditions............................. 2
Condition 1
    type..................................... Client-count
    value.................................... 10
Condition 2
    type..................................... Duration
    value (seconds).......................... 2000
Condition 3
    type..................................... Managed-ssid
    value.................................... Enabled
Condition 4
    type..................................... No-encryption
    value.................................... Enabled
Condition 5
    type..................................... Rssi
    value (dBm).............................. -50
Condition 6
    type..................................... Ssid
    SSID Count............................... 1
    SSID 1................................... test
```

Related Commands

config rogue rule

show rogue ignore-list

show rogue rule summary

show rogue rule summary

To display the rogue classification rules that are configured on the controller, use the **show rogue rule summary** command.

show rogue rule summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a list of all rogue rules that are configured on the controller:

```
(Cisco Controller) > show rogue rule summary
Priority Rule Name                State    Type          Match Hit Count
-------- ---------------------- -------- ------------- ----- ---------
1        mtest                  Enabled  Malicious     All   0
2        asdfasdf               Enabled  Malicious     All   0
```

The following example shows how to display a list of all rogue rules that are configured on the controller:

```
(Cisco Controller) > show rogue rule summary
Priority         Rule Name                 Rule state Class Type   Notify
   State    Match Hit Count
-------- ------------------------------ ----------- ----------- --------
 -------- ------ ---------
1        rule2                           Enabled    Friendly     Global
   Alert    All    234
2        rule1                           Enabled    Custom       Global
   Alert    All    0
```

Related Commands

config rogue rule

show rogue ignore-list

show rogue rule detailed

show tacacs acct statistics

To display detailed radio frequency identification (RFID) information for a specified tag, use the **show tacacs acct statistics** command.

show tacacs acct 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 display detailed RFID information:

```
(Cisco Controller) > show tacacs acct statistics
Accounting Servers:
Server Index..................................... 1
Server Address................................... 10.0.0.0
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 1
Retry Requests................................... 0
Accounting Response.............................. 0
Accounting Request Success....................... 0
Accounting Request Failure....................... 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. -1
Timeout Requests................................. 1
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

show tacacs athr statistics

To display TACACS+ server authorization statistics, use the **show tacacs athr statistics** command.

show tacacs athr 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 display TACACS server authorization statistics:

```
(Cisco Controller) > show tacacs athr statistics
Authorization Servers:
Server Index..................................... 3
Server Address................................... 10.0.0.3
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 0
Retry Requests................................... 0
Received Responses............................... 0
Authorization Success............................ 0
Authorization Failure............................ 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Related Commands

config tacacs acct

config tacacs athr

config tacacs auth

show tacacs auth statistics

show tacacs summary

show tacacs auth statistics

To display TACACS+ server authentication statistics, use the **show tacacs auth statistics** command.

show tacacs auth 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 display TACACS server authentication statistics:

```
(Cisco Controller) > show tacacs auth statistics
Authentication Servers:
Server Index..................................... 2
Server Address................................... 10.0.0.2
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 0
Retry Requests................................... 0
```

```
Accept Responses.............................. 0
Reject Responses.............................. 0
Error Responses............................... 0
Restart Responses............................. 0
Follow Responses.............................. 0
GetData Responses............................. 0
Encrypt no secret Responses................... 0
Challenge Responses........................... 0
Malformed Msgs................................ 0
Bad Authenticator Msgs........................ 0
Pending Requests.............................. 0
Timeout Requests.............................. 0
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

show tacacs summary

To display TACACS+ server summary information, use the **show tacacs summary** command.

show tacacs summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display TACACS server summary information:

```
(Cisco Controller) > show tacacs summary
Authentication Servers
Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
2    10.0.0.1         49       Enabled   30
Accounting Servers
Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.0.0.0         49      Enabled    5
Authorization Servers
Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
3    10.0.0.3         49       Enabled   5
Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
4    2001:9:6:40::623  49       Enabled   5
...
```

Related Commands

config tacacs acct

config tacacs athr

config tacacs auth

show tacacs summary

show tacacs athr statistics

show tacacs auth statistics

config Commands

This section lists the **config** commands to configure security settings for the controller.

config 802.11b preamble

To change the 802.11b preamble as defined in subclause 18.2.2.2 to **long** (slower, but more reliable) or **short** (faster, but less reliable), use the **config 802.11b preamble** command.

config 802.11b preamble {**long** | **short**}

Syntax Description

long	Specifies the long 802.11b preamble.
short	Specifies the short 802.11b preamble.

Command Default

The default 802.11b preamble value is short.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Note You must reboot the Cisco Wireless LAN Controller (reset system) with save to implement this command.

This parameter must be set to **long** to optimize this Cisco wireless LAN controller for some clients, including SpectraLink NetLink telephones.

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

The following example shows how to change the 802.11b preamble to short:

```
(Cisco Controller) >config 802.11b preamble short
(Cisco Controller) >(reset system with save)
```

config aaa auth

To configure the AAA authentication search order for management users, use the **config aaa auth** command.

config aaa auth mgmt [*aaa_server_type1* | *aaa_server_type2*]

Syntax Description

mgmt	Configures the AAA authentication search order for controller management users by specifying up to three AAA authentication server types. The order that the server types are entered specifies the AAA authentication search order.

aaa_server_type	(Optional) AAA authentication server type (**local**, **radius**, or **tacacs**). The **local** setting specifies the local database, the **radius** setting specifies the RADIUS server, and the **tacacs** setting specifies the TACACS+ server.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

You can enter two AAA server types as long as one of the server types is **local**. You cannot enter **radius** and **tacacs** together.

The following example shows how to configure the AAA authentication search order for controller management users by the authentication server type local:

```
(Cisco Controller) > config aaa auth radius local
```

Related Commands

show aaa auth

config aaa auth mgmt

To configure the order of authentication when multiple databases are configured, use the **config aaa auth mgmt** command.

config aaa auth mgmt [**radius** | **tacacs**]

Syntax Description

radius	(Optional) Configures the order of authentication for RADIUS servers.
tacacs	(Optional) Configures the order of authentication for TACACS servers.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the order of authentication for the RADIUS server:

```
(Cisco Controller) > config aaa auth mgmt radius
```

The following example shows how to configure the order of authentication for the TACACS server:

```
(Cisco Controller) > config aaa auth mgmt tacacs
```

Related Commands **show aaa auth order**

config auth-list add

To create an authorized access point entry, use the **config auth-list add** command.

config auth-list add {**mic** | **ssc**} *AP_MAC* [*AP_key*]

Syntax Description

mic	Specifies that the access point has a manufacture-installed certificate.
ssc	Specifies that the access point has a self-signed certificate.
AP_MAC	MAC address of a Cisco lightweight access point.
AP_key	(Optional) Key hash value that is equal to 20 bytes or 40 digits.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to create an authorized access point entry with a manufacturer-installed certificate on MAC address 00:0b:85:02:0d:20:

```
(Cisco Controller) > config auth-list add 00:0b:85:02:0d:20
```

Related Commands **config auth-list delete**

config auth-list ap-policy

config auth-list ap-policy

To configure an access point authorization policy, use the **config auth-list ap-policy** command.

config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **ssc** {**enable** | **disable**}}

Syntax Description

authorize-ap enable	Enables the authorization policy.
authorize-ap disable	Disables the AP authorization policy.
ssc enable	Allows the APs with self-signed certificates to connect.
ssc disable	Disallows the APs with self-signed certificates to connect.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable an access point authorization policy:

```
(Cisco Controller) > config auth-list ap-policy authorize-ap enable
```

The following example shows how to enable an access point with a self-signed certificate to connect:

```
(Cisco Controller) > config auth-list ap-policy ssc disable
```

Related Commands

config auth-list delete

config auth-list add

config auth-list delete

To delete an access point entry, use the **config auth-list delete** command.

config auth-list delete *AP_MAC*

Syntax Description

AP_MAC	MAC address of a Cisco lightweight access point.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to delete an access point entry for MAC address 00:1f:ca:cf:b6:60:

```
(Cisco Controller) > config auth-list delete 00:1f:ca:cf:b6:60
```

Related Commands

config auth-list delete

config auth-list add

config auth-list ap-policy

config advanced eap

To configure advanced extensible authentication protocol (EAP) settings, use the **config advanced eap** command.

config advanced eap {**bcast-key-interval** *seconds* | **eapol-key-timeout** *timeout* | **eapol-key-retries** *retries* | **identity-request-timeout** *timeout* | **identity-request-retries** *retries* | **key-index** *index* |

max-login-ignore-identity-response {**enable** | **disable**} **request-timeout** *timeout* | **request-retries** *retries*} }

Syntax Description

bcast-key-interval *seconds*	Specifies the EAP-broadcast key renew interval time in seconds. The range is from 120 to 86400 seconds.
eapol-key-timeout *timeout*	Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK. The default value is 1000 milliseconds.
eapol-key-retries *retries*	Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
identity-request- timeout *timeout*	Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client. The default value is 30 seconds.
identity-request- retries	Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
key-index *index*	Specifies the key index (0 or 3) used for dynamic wired equivalent privacy (WEP).
max-login-ignore- identity-response	When enabled, this command ignores the limit set for the number of devices that can be connected to the controller with the same username using 802.1xauthentication. When disabled, this command limits the number of devices that can be connected to the controller with the same username. This option is not applicable for Web auth user. Use the command **config netuser maxUserLogin** to set the limit of maximum number of devices per same username
enable	Ignores the same username reaching the maximum EAP identity response.
disable	Checks the same username reaching the maximum EAP identity response.

request-timeout	For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client. The default value is 30 seconds.
request-retries	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client. The default value is 2.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the key index used for dynamic wired equivalent privacy (WEP):

```
(Cisco Controller) > config advanced eap key-index 0
```

config advanced timers auth-timeout

To configure the authentication timeout, use the **config advanced timers auth-timeout** command.

config advanced timers auth-timeout *seconds*

Syntax Description

seconds	Authentication response timeout value in seconds between 10 and 600.

Command Default

The default authentication timeout value is 10 seconds.

Command History

Release	Modification
8.3	This command was introduced.

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

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

config advanced timers eap-timeout

To configure the Extensible Authentication Protocol (EAP) expiration timeout, use the **config advanced timers eap-timeout** command.

config advanced timers eap-timeout *seconds*

Syntax Description		
	seconds	EAP timeout value in seconds between 8 and 120.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the EAP expiration timeout to 10 seconds:

```
(Cisco Controller) >config advanced timers eap-timeout 10
```

config advanced timers eap-identity-request-delay

To configure the advanced Extensible Authentication Protocol (EAP) identity request delay in seconds, use the **config advanced timers eap-identity-request-delay** command.

config advanced timers eap-identity-request-delay *seconds*

Syntax Description		
	seconds	Advanced EAP identity request delay in number of seconds between 0 and 10.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the advanced EAP identity request delay to 8 seconds:

```
(Cisco Controller) >config advanced timers eap-identity-request-delay 8
```

config database size

To configure the local database, use the **config database size** command.

config database size *count*

Syntax Description		
	count	Database size value between 512 and 2040

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines Use the **show database** command to display local database configuration.

The following example shows how to configure the size of the local database:

```
(Cisco Controller) > config database size 1024
```

Related Commands **show database**

config exclusionlist

To create or delete an exclusion list entry, use the **config exclusionlist** command.

config exclusionlist {**add** *MAC* [*description*] | **delete** *MAC* | **description** *MAC* [*description*]}

Syntax Description

config exclusionlist	Configures the exclusion list.
add	Creates a local exclusion-list entry.
delete	Deletes a local exclusion-list entry
description	Specifies the description for an exclusion-list entry.
MAC	MAC address of the local Excluded entry.
description	(Optional) Description, up to 32 characters, for an excluded entry.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to create a local exclusion list entry for the MAC address *xx:xx:xx:xx:xx:xx:*

```
(Cisco Controller) > config exclusionlist add xx:xx:xx:xx:xx:xx lab
```

The following example shows how to delete a local exclusion list entry for the MAC address *xx:xx:xx:xx:xx:xx:*

```
(Cisco Controller) > config exclusionlist delete xx:xx:xx:xx:xx:xx lab
```

Related Commands **show exclusionlist**

config local-auth active-timeout

To specify the amount of time in which the controller attempts to authenticate wireless clients using local Extensible Authentication Protocol (EAP) after any pair of configured RADIUS servers fails, use the **config local-auth active-timeout** command.

config local-auth active-timeout *timeout*

Syntax Description

timeout	Timeout measured in seconds. The range is from 1 to 3600.

Command Default

The default timeout value is 100 seconds.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to specify the active timeout to authenticate wireless clients using EAP to 500 seconds:

```
(Cisco Controller) > config local-auth active-timeout 500
```

Related Commands

clear stats local-auth

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

config local-auth eap-profile

To configure local Extensible Authentication Protocol (EAP) authentication profiles, use the **config local-auth eap-profile** command.

config local-auth eap-profile {[**add** | **delete**] *profile_name* | **cert-issuer** {**cisco** | **vendor**} | **method** *method* **local-cert** {**enable** | **disable**} *profile_name* | **method** *method* **client-cert** {**enable** | **disable**} *profile_name* | **method** *method* **peer-verify ca-issuer** {**enable** | **disable**} | **method** *method* **peer-verify cn-verify** {**enable** | **disable**} | **method** *method* **peer-verify date-valid** {**enable** | **disable**}

Syntax Description

add	(Optional) Specifies that an EAP profile or method is being added.
delete	(Optional) Specifies that an EAP profile or method is being deleted.
profile_name	EAP profile name (up to 63 alphanumeric characters). Do not include spaces within a profile name.

cert-issuer	(For use with EAP-TLS, PEAP, or EAP-FAST with certificates) Specifies the issuer of the certificates that will be sent to the client. The supported certificate issuers are Cisco or a third-party vendor.
cisco	Specifies the Cisco certificate issuer.
vendor	Specifies the third-party vendor.
method	Configures an EAP profile method.
method	EAP profile method name. The supported methods are leap, fast, tls, and peap.
local-cert	(For use with EAP-FAST) Specifies whether the device certificate on the controller is required for authentication.
enable	Specifies that the parameter is enabled.
disable	Specifies that the parameter is disabled.
client-cert	(For use with EAP-FAST) Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.
peer-verify	Configures the peer certificate verification options.
ca-issuer	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the incoming certificate from the client is to be validated against the Certificate Authority (CA) certificates on the controller.
cn-verify	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates' CN on the controller.
date-valid	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to create a local EAP profile named FAST01:

```
(Cisco Controller) > config local-auth eap-profile add FAST01
```

The following example shows how to add the EAP-FAST method to a local EAP profile:

```
(Cisco Controller) > config local-auth eap-profile method add fast FAST01
```

The following example shows how to specify Cisco as the issuer of the certificates that will be sent to the client for an EAP-FAST profile:

```
(Cisco Controller) > config local-auth eap-profile method fast cert-issuer cisco
```

The following example shows how to specify that the incoming certificate from the client be validated against the CA certificates on the controller:

```
(Cisco Controller) > config local-auth eap-profile method fast peer-verify ca-issuer enable
```

Related Commands

config local-auth active-timeout

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

config local-auth method fast

To configure an EAP-FAST profile, use the **config local-auth method fast** command.

config local-auth method fast {**anon-prov** [**enable** | **disable**] | **authority-id** *auth_id* **pac-ttl** *days* | **server-key** *key_value*}

Syntax Description

anon-prov	Configures the controller to allow anonymous provisioning, which allows PACs to be sent automatically to clients that do not have one during Protected Access Credentials (PAC) provisioning.
enable	(Optional) Specifies that the parameter is enabled.
disable	(Optional) Specifies that the parameter is disabled.
authority-id	Configures the authority identifier of the local EAP-FAST server.
auth_id	Authority identifier of the local EAP-FAST server (2 to 32 hexadecimal digits).
pac-ttl	Configures the number of days for the Protected Access Credentials (PAC) to remain viable (also known as the time-to-live [TTL] value).
days	Time-to-live value (TTL) value (1 to 1000 days).

server-key	Configures the server key to encrypt or decrypt PACs.
key_value	Encryption key value (2 to 32 hexadecimal digits).

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to disable the controller to allows anonymous provisioning:

```
(Cisco Controller) > config local-auth method fast anon-prov disable
```

The following example shows how to configure the authority identifier 0125631177 of the local EAP-FAST server:

```
(Cisco Controller) > config local-auth method fast authority-id 0125631177
```

The following example shows how to configure the number of days to 10 for the PAC to remain viable:

```
(Cisco Controller) > config local-auth method fast pac-ttl 10
```

Related Commands

clear stats local-auth

config local-auth eap-profile

config local-auth active-timeout

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config local-auth user-credentials

To configure the local Extensible Authentication Protocol (EAP) authentication database search order for user credentials, use the **config local-auth user credentials** command.

config local-auth user-credentials {**local** [**ldap**] | **ldap** [**local**] }

Syntax Description

local	Specifies that the local database is searched for the user credentials.
ldap	(Optional) Specifies that the Lightweight Directory Access Protocol (LDAP) database is searched for the user credentials.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines The order of the specified database parameters indicate the database search order.

The following example shows how to specify the order in which the local EAP authentication database is searched:

```
(Cisco Controller) > config local-auth user credentials local lda
```

In the above example, the local database is searched first and then the LDAP database.

Related Commands

clear stats local-auth

config local-auth eap-profile

config local-auth method fast

config local-auth active-timeout

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

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 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 controller 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 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 radius acct

To configure settings for a RADIUS accounting server for the Cisco wireless LAN controller, use the **config radius acct** command.

config radius acct { {**add** *index IP addr port* {**ascii** | **hex**} *secret*} | **delete** *index* | **disable** *index* | **enable** *index* | **disable** *index* | **enable** *index* | {**mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen**}} | {**network** *index* {**disable** | **enable**}} | {**region** {**group** | **none** | **provincial**}} | **retransmit-timeout** *index seconds* | **realm** {**add** | **delete**} *index realm-string*}

Syntax Description

add	Adds a RADIUS accounting server (IPv4 or IPv6).
index	RADIUS server index (1 to 17).
IP addr	RADIUS server IP address (IPv4 or IPv6).
port	RADIUS server's UDP port number for the interface protocols.
ascii	Specifies the RADIUS server's secret type: **ascii**.
hex	Specifies the RADIUS server's secret type: **hex**.
secret	RADIUS server's secret.
enable	Enables a RADIUS accounting server.
disable	Disables a RADIUS accounting server.
delete	Deletes a RADIUS accounting server.
disable	Disables IPSec support for an accounting server.
enable	Enables IPSec support for an accounting server.
mac-delimiter	Configures MAC delimiter for caller station ID and calling station ID.
colon	Sets the delimiter to colon (For example: xx:xx:xx:xx:xx:xx).
hyphen	Sets the delimiter to hyphen (For example: xx-xx-xx-xx-xx-xx).
none	Disables delimiters (For example: xxxxxxxxxx).

single-hyphen	Sets the delimiters to single hyphen (For example: xxxxxx-xxxxxx).
network	Configures a default RADIUS server for network users.
group	Specifies RADIUS server type group.
none	Specifies RADIUS server type none.
provincial	Specifies RADIUS server type provincial.
retransmit-timeout	Changes the default retransmit timeout for the server.
seconds	The number of seconds between retransmissions.
realm	Specifies radius acct realm.
add	Adds radius acct realm.
delete	Deletes radius acct realm.

Command Default

When adding a RADIUS server, the port number defaults to 1813 and the state is **enabled**.

Usage Guidelines

IPSec is not supported for IPv6.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure a priority 1 RADIUS accounting server at *10.10.10.10* using port *1813* with a login password of *admin*:

```
(Cisco Controller) > config radius acct add 1 10.10.10.10 1813 ascii admin
```

The following example shows how to configure a priority 1 RADIUS accounting server at *2001:9:6:40::623* using port *1813* with a login password of *admin*:

```
(Cisco Controller) > config radius acct add 1 2001:9:6:40::623 1813 ascii admin
```

Related Topics

show radius acct statistics, on page 318

config radius acct mac-delimiter

To specify the delimiter to be used in the MAC addresses that are sent to the RADIUS accounting server, use the **config radius acct mac-delimiter** command.

config radius acct mac-delimiter {**colon** | **hyphen** | **single-hyphen** | **none**}

Syntax Description

colon	Sets the delimiter to a colon (for example, xx:xx:xx:xx:xx:xx).
hyphen	Sets the delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx).
single-hyphen	Sets the delimiter to a single hyphen (for example, xxxxxx-xxxxxx).
none	Disables the delimiter (for example, xxxxxxxxxxxx).

Command Default

The default delimiter is a hyphen.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to set the delimiter hyphen to be used in the MAC addresses that are sent to the RADIUS accounting server for the network users:

```
(Cisco Controller) > config radius acct mac-delimiter hyphen
```

Related Commands

show radius acct statistics

config radius acct network

To configure a default RADIUS server for network users, use the **config radius acct network** command.

config radius acct network *index* {**enable** | **disable**}

Syntax Description

index	RADIUS server index.
enable	Enables the server as a network user's default RADIUS server.
disable	Disables the server as a network user's default RADIUS server.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure a default RADIUS accounting server for the network users with RADIUS server index1:

```
(Cisco Controller) > config radius acct network 1 enable
```

Related Commands **show radius acct statistics**

config radius acct realm

To configure realm on RADIUS accounting server, use the **config radius acct realm** command.

config radius acct realm {**add** | **delete**} *radius_index realm_string*

Syntax Description

radius_server	Radius server index. The range is from 1 to 17.
add	Add realm to RADIUS accounting server.
delete	Delete realm from RADIUS accounting server.
realm_string	Unique string associated to RADIUS accounting realm.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how add realm to the RADIUS accounting server:

```
(Cisco Controller) > config radius acct realm add 3 test
```

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

To configure settings for a RADIUS authentication server for the Cisco wireless LAN controller, use the **config radius auth** command.

config radius auth {**add** *index IP addr portascii/hexsecret*} | | **delete** *index* | **disable** *index* | **enable** *index* | **framed-mtu** *mtu* | { **ipsec** {**authentication** {**hmac-md5** *index* | **hmac-sha1** *index* } | **disable** *index* | **enable** *index* | **encryption** {**256-aes** | **3des** | **aes** | **des**} *index* | **ike** {**auth-mode** {**pre-shared-key** *index ascii/hex shared_secret* | **certificate** *index* } | **dh-group** { **2048bit-group-14** | **group-1** | **group-2** | **group-5**} *index* | **lifetime** *seconds index* | **phase1** {**aggressive** | **main**} *index* } } | { { **keywrap**{**add** *ascii/hex kek mack index* } | **delete** *index* | **disable** | **enable**} } | {**mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen**} } | {{**management** *index* {**enable** | **disable**} } | { **mgmt-retransmit-timeout** *index Retransmit Timeout* } | { **network** *index* {**enable** | **disable**} } | {**realm** {**add** | **delete**} *radius-index realm-string*} } | {**region** {**group** | **none** | **provincial**} } | {**retransmit-timeout** *index Retransmit Timeout*} | { **rfc3576** {**enable** | **disable**} *index* }

Syntax Description

enable	Enables a RADIUS authentication server.
disable	Disables a RADIUS authentication server.
delete	Deletes a RADIUS authentication server.
index	RADIUS server index. The controller begins the search with 1. The server index range is from 1 to 17.
add	Adds a RADIUS authentication server. See the “Defaults” section.
IP addr	IP address (IPv4 or IPv6) of the RADIUS server.
port	RADIUS server’s UDP port number for the interface protocols.
ascii/hex	Specifies RADIUS server’s secret type: **ascii** or **hex**.
secret	RADIUS server’s secret.
callStationIdType	Configures Called Station Id information sent in RADIUS authentication messages.
framed-mtu	Configures the Framed-MTU for all the RADIUS servers. The framed-mtu range is from 64 to 1300 bytes.
ipsec	Enables or disables IPSEC support for an authentication server. **Note** IPSec is not supported for IPv6.
keywrap	Configures RADIUS keywrap.

ascii/hex	Specifies the input format of the keywrap keys.
kek	Enters the 16-byte key-encryption-key.
mack	Enters the 20-byte message-authenticator-code-key.
mac-delimiter	Configures MAC delimiter for caller station ID and calling station ID.
management	Configures a RADIUS Server for management users.
mgmt-retransmit-timeout	Changes the default management login retransmission timeout for the server.
network	Configures a default RADIUS server for network users.
realm	Configures radius auth realm.
region	Configures RADIUS region property.
retransmit-timeout	Changes the default network login retransmission timeout for the server.
rfc3576	Enables or disables RFC-3576 support for an authentication server.

Command Default

When adding a RADIUS server, the port number defaults to 1812 and the state is **enabled**.

Usage Guidelines

IPSec is not supported for IPv6.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure a priority *3* RADIUS authentication server at *10.10.10.10* using port *1812* with a login password of *admin*:

```
(Cisco Controller) > config radius auth add 3 10.10.10.10 1812 ascii admin
```

The following example shows how to configure a priority *3* RADIUS authentication server at *2001:9:6:40::623* using port *1812* with a login password of *admin*:

```
(Cisco Controller) > config radius auth add 3 2001:9:6:40::623 1812 ascii admin
```

Related Topics

show radius auth statistics, on page 320

config radius auth callStationIdType

To configure the RADIUS authentication server, use the **config radius auth callStationIdType** command.

config radius auth callStationIdType {**ap-ethmac-only** | **ap-ethmac-ssid** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddr-only** | **ap-macaddr-ssid** | **ap-name** | **ap-name-ssid** | **flex-group-name** | **ipaddr** | **macaddr** | **vlan-id**}

Syntax Description

ipaddr	Configures the Call Station ID type to use the IP address (only Layer 3).
macaddr	Configures the Call Station ID type to use the system's MAC address (Layers 2 and 3).
ap-macaddr-only	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3).
ap-macaddr-ssid	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3) in the format *AP MAC address*:*SSID*.
ap-ethmac-only	Configures the Called Station ID type to use the access point's Ethernet MAC address.
ap-ethmac-ssid	Configures the Called Station ID type to use the access point's Ethernet MAC address in the format *AP Ethernet MAC address*:*SSID*.
ap-group-name	Configures the Call Station ID type to use the AP group name. If the AP is not part of any AP group, default-group is taken as the AP group name.
flex-group-name	Configures the Call Station ID type to use the FlexConnect group name. If the FlexConnect AP is not part of any FlexConnect group, the system MAC address is taken as the Call Station ID.
ap-name	Configures the Call Station ID type to use the access point's name.
ap-name-ssid	Configures the Call Station ID type to use the access point's name in the format *AP name*:*SSID*
ap-location	Configures the Call Station ID type to use the access point's location.
vlan-id	Configures the Call Station ID type to use the system's VLAN-ID.
ap-label-address	Configures the Call Station ID type to the AP MAC address that is printed on the AP label, for the accounting messages.
ap-label-address-ssid	Configures the Call Station ID type to the AP MAC address:SSID format.

Command Default

The MAC address of the system.

Usage Guidelines

The controller sends the Called Station ID attribute to the RADIUS server in all authentication and accounting packets. The Called Station ID attribute can be used to classify users to different groups based on the attribute value. The command is applicable only for the Called Station and not for the Calling Station.

You cannot send only the SSID as the Called-Station-ID, you can only combine the SSID with either the access point MAC address or the access point name.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the call station ID type to use the IP address:

```
(Cisco Controller) > config radius auth callStationIdType ipAddr
```

The following example shows how to configure the call station ID type to use the system's MAC address:

```
(Cisco Controller) > config radius auth callStationIdType macAddr
```

The following example shows how to configure the call station ID type to use the access point's MAC address:

```
(Cisco Controller) > config radius auth callStationIdType ap-macAddr
```

config radius auth keywrap

To enable and configure Advanced Encryption Standard (AES) key wrap, which makes the shared secret between the controller and the RADIUS server more secure, use the **config radius auth keywrap** command.

config radius auth keywrap {**enable** | **disable** | **add** {**ascii** | **hex**} *kek mack* | **delete**} *index*

Syntax Description

enable	Enables AES key wrap.
disable	Disables AES key wrap.
add	Configures AES key wrap attributes.
ascii	Configures key wrap in an ASCII format.
hex	Configures key wrap in a hexadecimal format.
kek	16-byte Key Encryption Key (KEK).
mack	20-byte Message Authentication Code Key (MACK).
delete	Deletes AES key wrap attributes.
index	Index of the RADIUS authentication server on which to configure the AES key wrap.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the AES key wrap for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth keywrap enable
```

Related Commands **show radius auth statistics**

config radius auth mac-delimiter

To specify a delimiter to be used in the MAC addresses that are sent to the RADIUS authentication server, use the **config radius auth mac-delimiter** command.

config radius auth mac-delimiter {**colon** | **hyphen** | **single-hyphen** | **none**}

Syntax Description

colon	Sets a delimiter to a colon (for example, xx:xx:xx:xx:xx:xx).
hyphen	Sets a delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx).
single-hyphen	Sets a delimiter to a single hyphen (for example, xxxxxx-xxxxxx).
none	Disables the delimiter (for example, xxxxxxxxxxxx).

Command Default The default delimiter is a hyphen.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to specify a delimiter hyphen to be used for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth mac-delimiter hyphen
```

Related Commands **show radius auth statistics**

config radius auth management

To configure a default RADIUS server for management users, use the **config radius auth management** command.

config radius auth management *index* {**enable** | **disable**}

Syntax Description

index	RADIUS server index.
enable	Enables the server as a management user's default RADIUS server.
disable	Disables the server as a management user's default RADIUS server.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure a RADIUS server for management users:

```
(Cisco Controller) > config radius auth management 1 enable
```

Related Commands

show radius acct statistics

config radius acct network

config radius auth mgmt-retransmit-timeout

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 network

To configure a default RADIUS server for network users, use the **config radius auth network** command.

config radius auth network *index* {**enable** | **disable**}

Syntax Description

index	RADIUS server index.
enable	Enables the server as a network user default RADIUS server.
disable	Disables the server as a network user default RADIUS server.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure a default RADIUS server for network users:

```
(Cisco Controller) > config radius auth network 1 enable
```

Related Commands

show radius acct statistics

config radius acct network

config radius auth realm

To configure realm on RADIUS authentication server, use the **config radius auth realm** command.

config radius auth realm {**add** | **delete**} *radius_index realm_string*

Syntax Description

radius_server	Radius server index. The range is from 1 to 17.
add	Add realm to RADIUS authentication server.
delete	Delete realm from RADIUS authentication server.
realm_string	Unique string associated to RADIUS authentication realm.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how add realm to the RADIUS authentication server:

```
(Cisco Controller) > config radius auth realm add 3 test
```

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 rfc3576

To configure RADIUS RFC-3576 support for the authentication server for the controller, use the **config radius auth rfc3576** command.

config radius auth rfc3576 { **enable** | **disable** } *index*

Syntax Description

enable	Enables RFC-3576 support for an authentication server.
disable	Disables RFC-3576 support for an authentication server.
index	RADIUS server index.

Command Default

Disabled

Command History

Release	Modification
8.7	This command was introduced.

Usage Guidelines

RFC 3576, which is an extension to the RADIUS protocol, allows dynamic changes to a user session. RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session. Disconnect messages cause a user session to be terminated immediately; CoA messages modify session authorization attributes such as data filters.

The following example shows how to enable the RADIUS RFC-3576 support for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth rfc3576 enable 2
```

Related Commands

show radius auth statistics

show radius summary

show radius rfc3576

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 radius aggressive-failover disabled

To configure the controller to mark a RADIUS server as down (not responding) after the server does not reply to three consecutive clients, use the **config radius aggressive-failover disabled** command.

config radius aggressive-failover disabled

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 mark a RADIUS server as down:

```
(Cisco Controller) > config radius aggressive-failover disabled
```

Related Commands **show radius summary**

config radius backward compatibility

To configure RADIUS backward compatibility for the Cisco wireless LAN controller, use the **config radius backward compatibility** command.

config radius backward compatibility {**enable** | **disable**}

Syntax Description

enable	Enables RADIUS vendor ID backward compatibility.
disable	Disables RADIUS vendor ID backward compatibility.

Command Default Enabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the RADIUS backward compatibility settings:

```
(Cisco Controller) > config radius backward compatibility disable
```

Related Commands **show radius summary**

config radius callStationIdCase

To configure callStationIdCase information sent in RADIUS messages for the controller, use the **config radius callStationIdCase** command.

config radius callStationIdCase { **legacy** | **lower** | **upper** }

Syntax Description

legacy	Configures Call Station IDs for Layer 2 authentication to RADIUS in uppercase.
lower	Configures all Call Station IDs to RADIUS in lowercase.
upper	Configures all Call Station IDs to RADIUS in uppercase.

Command Default

Enabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to send the call station ID in lowercase:

```
(Cisco Controller) > config radius callStationIdCase lower
```

Related Commands

show radius summary

config radius callStationIdType

To configure the Called Station ID type information sent in RADIUS accounting messages for the Cisco wireless LAN controller, use the **config radius callStationIdType** command.

config radius callStationIdType {**ap-ethmac-only** | **ap-ethmac-ssid** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddr-only** | **ap-macaddr-ssid** | **ap-name** | **ap-name-ssid** | **flex-group-name** | **ipaddr** | **macaddr** | **vlan-id**}

Syntax Description

ipaddr	Configures the Call Station ID type to use the IP address (only Layer 3).
macaddr	Configures the Call Station ID type to use the system's MAC address (Layers 2 and 3).
ap-macaddr-only	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3).
ap-macaddr-ssid	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3) in the format *AP MAC address*:*SSID*.
ap-ethmac-only	Configures the Called Station ID type to use the access point's Ethernet MAC address.
ap-ethmac-ssid	Configures the Called Station ID type to use the access point's Ethernet MAC address in the format *AP Ethernet MAC address*:*SSID*.

ap-group-name	Configures the Call Station ID type to use the AP group name. If the AP is not part of any AP group, default-group is taken as the AP group name.
flex-group-name	Configures the Call Station ID type to use the FlexConnect group name. If the FlexConnect AP is not part of any FlexConnect group, the system MAC address is taken as the Call Station ID.
ap-name	Configures the Call Station ID type to use the access point's name.
ap-name-ssid	Configures the Call Station ID type to use the access point's name in the format *AP name*:*SSID*
ap-location	Configures the Call Station ID type to use the access point's location.
ap-mac-ssid-ap-group	Sets Called Station ID type to the format <AP MAC address>:<SSID>:<AP Group>
vlan-id	Configures the Call Station ID type to use the system's VLAN-ID.
ap-label-address	Configures the Call Station ID type to the AP MAC address that is printed on the AP label, for the accounting messages.
ap-label-address-ssid	Configures the Call Station ID type to the AP MAC address:SSID format.

Command Default

The IP address of the system.

Usage Guidelines

The controller sends the Called Station ID attribute to the RADIUS server in all authentication and accounting packets. The Called Station ID attribute can be used to classify users to different groups based on the attribute value. The command is applicable only for the Called Station and not for the Calling Station.

You cannot send only the SSID as the Called-Station-ID, you can only combine the SSID with either the access point MAC address or the access point name.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the call station ID type to use the IP address:

```
(Cisco Controller) > config radius callStationIdType ipaddr
```

The following example shows how to configure the call station ID type to use the system's MAC address:

```
(Cisco Controller) > config radius callStationIdType macaddr
```

The following example shows how to configure the call station ID type to use the access point's MAC address:

```
(Cisco Controller) > config radius callStationIdType ap-macaddr-only
```

Related Topics

show radius summary, on page 321

config radius dns

To retrieve the RADIUS IP information from a DNS server, use the **config radius dns** command.

config radius dns { **global** *port* { *ascii* | *hex* } *secret* | **query** *url timeout* | **serverip** *ip_address* | **disable** | **enable** }

Syntax Description

global	Configures the global port and secret to retrieve the RADIUS IP information from a DNS server.
port	Port number for authentication. The range is from 1 to 65535. All the DNS servers should use the same authentication port.
ascii	Format of the shared secret that you should set to ASCII.
hex	Format of the shared secret that you should set to hexadecimal.
secret	RADIUS server login secret.
query	Configures the fully qualified domain name (FQDN) of the RADIUS server and DNS timeout.
url	FQDN of the RADIUS server. The FQDN can be up to 63 case-sensitive, alphanumeric characters.
timeout	Maximum time that the controller waits for, in days, before timing out the request and resending it. The range is from 1 to 180.
serverip	Configures the DNS server IP address.
ip_address	DNS server IP address.
disable	Disables the RADIUS DNS feature. By default, this feature is disabled.
enable	Enables the controller to retrieve the RADIUS IP information from a DNS server. When you enable a DNS query, the static configurations are overridden, that is, the DNS list overrides the static AAA list.

Command Default

You cannot configure the global port and secret to retrieve the RADIUS IP information.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The accounting port is derived from the authentication port. All the DNS servers should use the same secret.

The following example shows how to enable the RADIUS DNS feature on the controller:

```
(Cisco Controller) > config radius dns enable
```

Related Topics

config radius acct, on page 362
config radius auth, on page 366
config tacacs dns, on page 407
debug dns, on page 419

config radius fallback-test

To configure the RADIUS server fallback behavior, use the **config radius fallback-test** command.

config radius fallback-test mode {**off** | **passive** | **active**} | **username** *username*} | {**interval** *interval*}

Syntax Description

mode	Specifies the mode.
off	Disables RADIUS server fallback.
passive	Causes the controller to revert to a preferable server (with a lower server index) from the available backup servers without using extraneous probe messages. The controller ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
active	Causes the controller to revert to a preferable server (with a lower server index) from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller ignores all inactive servers for all active RADIUS requests.
username	Specifies the username.
username	Username. The username can be up to 16 alphanumeric characters.
interval	Specifies the probe interval value.
interval	Probe interval. The range is 180 to 3600.

Command Default

The default probe interval is 300.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to disable the RADIUS accounting server fallback behavior:

```
(Cisco Controller) > config radius fallback-test mode off
```

The following example shows how to configure the controller to revert to a preferable server from the available backup servers without using the extraneous probe messages:

```
(Cisco Controller) > config radius fallback-test mode passive
```

The following example shows how to configure the controller to revert to a preferable server from the available backup servers by using RADIUS probe messages:

```
(Cisco Controller) > config radius fallback-test mode active
```

Related Commands

config advanced probe filter

config advanced probe limit

show advanced probe

show radius acct statistics

config rogue adhoc

To globally or individually configure the status of an Independent Basic Service Set (IBSS or *ad-hoc*) rogue access point, use the **config rogue adhoc** command.

config rogue adhoc {**enable** | **disable** | **external** *rogue_MAC* | **alert** {*rogue_MAC* | **all**} | **auto-contain** [*monitor_ap*] | **contain** *rogue_MAC 1234_aps*| }

config rogue adhoc {**delete** {**all** | **mac-address** *mac-address*} | **classify** {**friendly state** {**external** | **internal**} *mac-address* | **malicious state** {**alert** | **contain**} *mac-address* | **unclassified state** {**alert** | **contain** } *mac-address*}

Syntax Description

enable	Globally enables detection and reporting of ad-hoc rogues.
disable	Globally disables detection and reporting of ad-hoc rogues.
external	Configure external state on the rogue access point that is outside the network and poses no threat to WLAN security. The controller acknowledges the presence of this rogue access point.
rogue_MAC	MAC address of the ad-hoc rogue access point.

alert	Generates an SMNP trap upon detection of the ad-hoc rogue, and generates an immediate alert to the system administrator for further action.
all	Enables alerts for all ad-hoc rogue access points.
auto-contain	Contains all wired ad-hoc rogues detected by the controller.
monitor_ap	(Optional) IP address of the ad-hoc rogue access point.
contain	Contains the offending device so that its signals no longer interfere with authorized clients.
1234_aps	Maximum number of Cisco access points assigned to actively contain the ad-hoc rogue access point (1 through 4, inclusive).
delete	Deletes ad-hoc rogue access points.
all	Deletes all ad-hoc rogue access points.
mac-address	Deletes ad-hoc rogue access point with the specified MAC address.
mac-address	MAC address of the ad-hoc rogue access point.
classify	Configures ad-hoc rogue access point classification.
friendly state	Classifies ad-hoc rogue access points as friendly.
internal	Configures alert state on rogue access point that is inside the network and poses no threat to WLAN security. The controller trusts this rogue access point.
malicious state	Classifies ad-hoc rogue access points as malicious.
alert	Configures alert state on the rogue access point that is not in the neighbor list or in the user configured friendly MAC list. The controller forwards an immediate alert to the system administrator for further action.
contain	Configures contain state on the rogue access point. Controller contains the offending device so that its signals no longer interfere with authorized clients.
unclassified state	Classifies ad-hoc rogue access points as unclassified.

Command Default

The default for this command is **enabled** and is set to **alert**. The default for auto-containment is **disabled**.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The controller continuously monitors all nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses RLDP to determine if the rogue is attached to your wired network.

Note RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS).

When you enter any of the containment commands, the following warning appears:

```
Using this feature may have legal consequences. Do you want to continue? (y/n) :
```

The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

Enter the **auto-contain** command with the *monitor_ap* argument to monitor the rogue access point without containing it. Enter the **auto-contain** command without the optional *monitor_ap* to automatically contain all wired ad-hoc rogues detected by the controller.

The following example shows how to enable the detection and reporting of ad-hoc rogues:

```
(Cisco Controller) > config rogue adhoc enable
```

The following example shows how to enable alerts for all ad-hoc rogue access points:

```
(Cisco Controller) > config rogue adhoc alert all
```

The following example shows how to classify an ad-hoc rogue access point as friendly and configure external state on it:

```
(Cisco Controller) > config rogue adhoc classify friendly state internal 11:11:11:11:11:11
```

Related Commands

config rogue auto-contain level

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap classify

To classify the status of a rogue access point, use the **config rogue ap classify** command.

config rogue ap classify {**friendly state** {**internal** | **external**} *ap_mac* }

config rogue ap classify {**malicious** | **unclassified**} **state** {**alert** | **contain**} *ap_mac*

Syntax Description

friendly	Classifies a rogue access point as friendly.
state	Specifies a response to classification.
internal	Configures the controller to trust this rogue access point.
external	Configures the controller to acknowledge the presence of this access point.
ap_mac	MAC address of the rogue access point.
malicious	Classifies a rogue access point as potentially malicious.
unclassified	Classifies a rogue access point as unknown.
alert	Configures the controller to forward an immediate alert to the system administrator for further action.
contain	Configures the controller to contain the offending device so that its signals no longer interfere with authorized clients.

Command Default

These commands are disabled by default. Therefore, all unknown access points are categorized as **unclassified** by default.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

A rogue access point cannot be moved to the unclassified class if its current state is contain.

When you enter any of the containment commands, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party’s network could have legal consequences.

The following example shows how to classify a rogue access point as friendly and can be trusted:

```
(Cisco Controller) > config rogue ap classify friendly state internal 11:11:11:11:11:11
```

The following example shows how to classify a rogue access point as malicious and to send an alert:

```
(Cisco Controller) > config rogue ap classify malicious state alert 11:11:11:11:11:11
```

The following example shows how to classify a rogue access point as unclassified and to contain it:

```
(Cisco Controller) > config rogue ap classify unclassified state contain 11:11:11:11:11:11
```

Related Commands

config rogue adhoc

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue ap timeout

config rogue ap valid-client

config rogue client

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 client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap friendly

To add a new friendly access point entry to the friendly MAC address list, or delete an existing friendly access point entry from the list, use the **config rogue ap friendly** command.

config rogue ap friendly {**add** | **delete**} *ap_mac*

Syntax Description

add	Adds this rogue access point from the friendly MAC address list.
delete	Deletes this rogue access point from the friendly MAC address list.
ap_mac	MAC address of the rogue access point that you want to add or delete.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a new friendly access point with MAC address 11:11:11:11:11:11 to the friendly MAC address list.

```
(Cisco Controller) > config rogue ap friendly add 11:11:11:11:11:11
```

Related Commands

config rogue adhoc

config rogue ap classify

config rogue ap rldp

config rogue ap ssid

config rogue ap timeout

config rogue ap valid-client

config rogue client

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 client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap rldp

To enable, disable, or initiate the Rogue Location Discovery Protocol (RLDP), use the **config rogue ap rldp** command.

config rogue ap rldp enable {**alarm-only** | **auto-contain**} [*monitor_ap_only*]

config rogue ap rldp initiate *rogue_mac_address*

config rogue ap rldp disable

Syntax Description

alarm-only	When entered without the optional argument *monitor_ap_only*, enables RLDP on all access points.

auto-contain	When entered without the optional argument *monitor_ap_only*, automatically contains all rogue access points.
monitor_ap_only	(Optional) RLDP is enabled (when used with **alarm-only** keyword), or automatically contained (when used with **auto-contain** keyword) is enabled only on the designated monitor access point.
initiate	Initiates RLDP on a specific rogue access point.
rogue_mac_address	MAC address of specific rogue access point.
disable	Disables RLDP on all access points.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When you enter any of the containment commands, the following warning appears: "Using this feature may have legal consequences. Do you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

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

```
(Cisco Controller) > config rogue ap rldp enable alarm-only
```

The following example shows how to enable RLDP on monitor-mode access point ap_1:

```
(Cisco Controller) > config rogue ap rldp enable alarm-only ap_1
```

The following example shows how to start RLDP on the rogue access point with MAC address 123.456.789.000:

```
(Cisco Controller) > config rogue ap rldp initiate 123.456.789.000
```

The following example shows how to disable RLDP on all access points:

```
(Cisco Controller) > config rogue ap rldp disable
```

Related Commands

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap ssid

config rogue ap timeout

config rogue ap valid-client

config rogue client

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 client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap ssid

To generate an alarm only, or to automatically contain a rogue access point that is advertising your network's service set identifier (SSID), use the **config rogue ap ssid** command.

config rogue ap ssid {**alarm** | **auto-contain**}

Syntax Description

alarm	Generates only an alarm when a rogue access point is discovered to be advertising your network's SSID.
auto-contain	Automatically contains the rogue access point that is advertising your network's SSID.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When you enter any of the containment commands, the following warning appears: "Using this feature may have legal consequences. Do you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

The following example shows how to automatically contain a rogue access point that is advertising your network's SSID:

```
(Cisco Controller) > config rogue ap ssid auto-contain
```

Related Commands

config rogue adhoc
config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap timeout
config rogue ap valid-client
config rogue client
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 client detailed
show rogue client summary
show rogue ignore-list
show rogue rule detailed
show rogue rule 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 rogue ap valid-client

To generate an alarm only, or to automatically contain a rogue access point to which a trusted client is associated, use the **config rogue ap valid-client** command.

config rogue ap valid-client {**alarm** | **auto-contain**}

Syntax Description

alarm	Generates only an alarm when a rogue access point is discovered to be associated with a valid client.
auto-contain	Automatically contains a rogue access point to which a trusted client is associated.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When you enter any of the containment commands, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial,

Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

The following example shows how to automatically contain a rogue access point that is associated with a valid client:

```
(Cisco Controller) > config rogue ap valid-client auto-contain
```

Related Commands

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

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 rogue client

To configure rogue clients, use the **config rogue client** command.

config rogue client {**aaa** {**enable** | **disable**} | **alert** *ap_mac* | **contain** *client_mac* | **delete** {**state** {**alert** | **any** | **contained** | **contained-pending**} | **all** | **mac-address** *client_mac*} | **mse** {**enable** | **disable**} } }

Syntax Description

aaa	Configures AAA server or local database to validate whether rogue clients are valid clients. The default is disabled.
enable	Enables the AAA server or local database to check rogue client MAC addresses for validity.
disable	Disables the AAA server or local database to check rogue client MAC addresses for validity.

alert	Configures the controller to forward an immediate alert to the system administrator for further action.
ap_mac	Access point MAC address.
contain	Configures the controller to contain the offending device so that its signals no longer interfere with authorized clients.
client_mac	MAC address of the rogue client.
delete	Deletes the rogue client.
state	Deletes the rogue clients according to their state.
alert	Deletes the rogue clients in alert state.
any	Deletes the rogue clients in any state.
contained	Deletes all rogue clients that are in contained state.
contained-pending	Deletes all rogue clients that are in contained pending state.
all	Deletes all rogue clients.
mac-address	Deletes a rogue client with the configured MAC address.
mse	Validates if the rogue clients are valid clients using MSE. The default is disabled.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

You cannot validate rogue clients against MSE and AAA at the same time.

The following example shows how to enable the AAA server or local database to check MAC addresses:

```
(Cisco Controller) > config rogue client aaa enable
```

The following example shows how to disable the AAA server or local database from checking MAC addresses:

```
(Cisco Controller) > config rogue client aaa disable
```

Related Commands

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue detection

To enable or disable rogue detection, use the **config rogue detection** command.

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

config rogue detection {**enable** | **disable**} {*cisco_ap* | **all**}

Syntax Description

enable	Enables rogue detection on this access point.
disable	Disables rogue detection on this access point.
cisco_ap	Cisco access point.
all	Specifies all access points.

Command Default

The default rogue detection value is enabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Rogue detection is enabled by default for all access points joined to the controller except for OfficeExtend access points. OfficeExtend access points are deployed in a home environment and are likely to detect a large number of rogue devices.

The following example shows how to enable rogue detection on the access point Cisco_AP:

```
(Cisco Controller) > config rogue detection enable Cisco_AP
```

Related Commands

config rogue rule

config trapflags rogueap

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue detection client-threshold

To configure the rogue client threshold for access points, use the **config rogue detection client-threshold** command.

config rogue detection client-threshold *value*

Syntax Description

value	Threshold rogue client count on an access point after which a trap is sent from the controller. The range is from 1 to 256. Enter 0 to disable the feature.

Command Default

The default rogue client threshold is 0.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the rogue client threshold:

```
(Cisco Controller) >config rogue detection client-threshold 200
```

Related Topics

config rogue detection min-rssi, on page 393
config rogue detection monitor-ap, on page 394
show rogue rule summary, on page 340
config rogue detection report-interval, on page 395
config rogue detection security-level, on page 396
config rogue detection transient-rogue-interval, on page 397

config rogue detection min-rssi

To configure the minimum Received Signal Strength Indicator (RSSI) value at which APs can detect rogues and create a rogue entry in the controller, use the **config rogue detection min-rssi** command.

config rogue detection min-rssi *rssi-in-dBm*

Syntax Description

rssi-in-dBm	Minimum RSSI value. The valid range is from –70 dBm to –128 dBm, and the default value is –128 dBm.

Command Default

The default RSSI value to detect rogues in APs is -128 dBm.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

This feature is applicable to all the AP modes.

There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.

The following example shows how to configure the minimum RSSI value:

```
(Cisco Controller) > config rogue detection min-rssi –80
```

Related Commands

config rogue detection

show rogue ap clients

config rogue rule

config trapflags rogueap

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue detection monitor-ap

To configure the rogue report interval for all monitor mode Cisco APs, use the **config rogue detection monitor-ap** command.

config rogue detection monitor-ap {**report-interval** | **transient-rogue-interval**} *time-in-seconds*

Syntax Description

report-interval	Specifies the interval at which rogue reports are sent.
transient-rogue-interval	Specifies the interval at which rogues are consistently scanned for by APs after the first time the rogues are scanned.
time-in-seconds	Time in seconds. The valid range is as follows: • 10 to 300 for **report-interval** • 120 to 1800 for **transient-rogue-interval**

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

This feature is applicable to APs that are in monitor mode only.

Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter the rogues based on their transient interval values.

This feature has the following advantages:

- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.
- Unnecessary memory allocation for transient rogues are avoided.

The following example shows how to configure the rogue report interval to 60 seconds:

```
(Cisco Controller) > config rogue detection monitor-ap report-interval 60
```

The following example shows how to configure the transient rogue interval to 300 seconds:

```
(Cisco Controller) > config rogue detection monitor-ap transient-rogue-interval 300
```

Related Commands

config rogue detection

config rogue detection min-rssi

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue detection report-interval

To configure the rogue detection report interval, use the **config rogue detection report-interval** command.

config rogue detection report-interval *time*

Syntax Description

time	Time interval, in seconds, at which the access points send the rogue detection report to the controller. The range is from 10 to 300.

Command Default

The default rogue detection report interval is 10 seconds.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

This feature is applicable only to the access points that are in the monitor mode.

The following example shows how to configure the rogue detection report interval:

```
(Cisco Controller) >config rogue detection report-interval 60
```

Related Topics

config rogue detection min-rssi, on page 393
config rogue detection monitor-ap, on page 394
show rogue rule summary, on page 340
config rogue detection client-threshold, on page 393
config rogue detection security-level, on page 396
config rogue detection transient-rogue-interval, on page 397

config rogue detection security-level

To configure the rogue detection security level, use the **config rogue detection security-level** command.

config rogue detection security-level {**critical** | **custom** | **high** | **low**}

Syntax Description

critical	Configures the rogue detection security level to critical.
custom	Configures the rogue detection security level to custom, and allows you to configure the rogue policy parameters.
high	Configures the rogue detection security level to high. This security level configures basic rogue detection and auto containment for medium-scale or less critical deployments. The Rogue Location Discovery Protocol (RLDP) is disabled for this security level.
low	Configures the rogue detection security level to low. This security level configures basic rogue detection for small-scale deployments. Auto containment is not supported for this security level.

Command Default

The default rogue detection security level is custom.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the rogue detection security level to high:

```
(Cisco Controller) > config rogue detection security-level high
```

Related Topics

config rogue detection min-rssi, on page 393
config rogue detection monitor-ap, on page 394
show rogue rule summary, on page 340
config rogue detection client-threshold, on page 393
config rogue detection report-interval, on page 395
config rogue detection transient-rogue-interval, on page 397

config rogue detection transient-rogue-interval

To configure the rogue-detection transient interval, use the **config rogue detection transient-rogue-interval** command.

config rogue detection transient-rogue-interval *time*

Syntax Description

time	Time interval, in seconds, at which a rogue should be consistently scanned by the access point after the rogue is scanned for the first time. The range is from 120 to 1800.

Command Default

The default rogue-detection transient interval for each security level is as follows:

- Low—120 seconds
- High—300 seconds
- Critical—600 seconds

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

This feature applies only to the access points that are in the monitor mode.

After the rogue is scanned consistently, updates are sent periodically to the controller. The access points filter the active transient rogues for a very short period and are then silent.

The following example shows how to configure the rogue detection transient interval:

```
(Cisco Controller) > config rogue detection transient-rogue-interval 200
```

Related Topics

config rogue detection min-rssi, on page 393
config rogue detection monitor-ap, on page 394
show rogue rule summary, on page 340
config rogue detection client-threshold, on page 393
config rogue detection report-interval, on page 395
config rogue detection security-level, on page 396

config rogue rule

To add and configure rogue classification rules, use the **config rogue rule** command.

config rogue rule {**add ap priority** *priority* **classify** {**custom** *severity-score classification-name* | **friendly** | **malicious**} **notify** {**all** | **global** | **none** | **local**} **state** {**alert** | **contain** | **delete** | **internal** | **external**} *rule_name* | **classify** {**custom** *severity-score classification-name* | **friendly** | **malicious**} *rule_name* | **condition ap** {**set** | **delete**} *condition_type condition_value rule_name* | {**enable** | **delete** | **disable**} {**all** | *rule_name*} | **match** {**all** | **any**} | **priority** *priority* | **notify** {**all** | **global** | **none** | **local**} *rule_name* | **state** {**alert** | **contain** | **internal** | **external**} *rule_name*}

Syntax Description

add ap priority	Adds a rule with match any criteria and the priority that you specify.
priority	Priority of this rule within the list of rules.
classify	Specifies the classification of a rule.
custom	Classifies devices matching the rule as custom.
severity-score	Custom classification severity score of the rule. The range is from 1 to 100.
classification-name	Custom classification name. The name can be up to 32 case-sensitive, alphanumeric characters.
friendly	Classifies a rule as friendly.
malicious	Classifies a rule as malicious.
notify	Configures type of notification upon rule match.
all	Notifies the controller and a trap receiver such as Cisco Prime Infrastructure.
global	Notifies only a trap receiver such as Cisco Prime Infrastructure.
local	Notifies only the controller.
none	Notifies neither the controller nor a trap receiver such as Cisco Prime Infrastructure.
state	Configures state of the rogue access point after a rule match.
alert	Configures alert state on the rogue access point that is not in the neighbor list or in the user configured friendly MAC list. The controller forwards an immediate alert to the system administrator for further action.
contain	Configures contain state on the rogue access point. Controller contains the offending device so that its signals no longer interfere with authorized clients.
delete	Configures delete state on the rogue access point.
external	Configures external state on the rogue access point that is outside the network and poses no threat to WLAN security. The controller acknowledges the presence of this rogue access point.
internal	Configures alert state on rogue access point that is inside the network and poses no threat to WLAN security. The controller trusts this rogue access point.

rule_name	Rule to which the command applies, or the name of a new rule.
condition ap	Specifies the conditions for a rule that the rogue access point must meet.
set	Adds conditions to a rule that the rogue access point must meet.
delete	Removes conditions to a rule that the rogue access point must meet.
condition_type	Type of the condition to be configured. The condition types are listed below: • client-count—Requires that a minimum number of clients be associated to a rogue access point. The valid range is 1 to 10 (inclusive). • duration—Requires that a rogue access point be detected for a minimum period of time. The valid range is 0 to 3600 seconds (inclusive). • managed-ssid—Requires that a rogue access point's SSID be known to the controller. • no-encryption—Requires that a rogue access point's advertised WLAN does not have encryption enabled. • rssi—Requires that a rogue access point have a minimum RSSI value. The range is from –95 to –50 dBm (inclusive). • ssid—Requires that a rogue access point have a specific SSID. • substring-ssid—Requires that a rogue access point have a substring of a user-configured SSID.
condition_value	Value of the condition. This value is dependent upon the condition_type. For instance, if the condition type is ssid, then the condition value is either the SSID name or all.
enable	Enables all rules or a single specific rule.
delete	Deletes all rules or a single specific rule.
disable	Deletes all rules or a single specific rule.

match	Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.
all	Specifies all rules defined.
any	Specifies any rule meeting certain criteria.
priority	Changes the priority of a specific rule and shifts others in the list accordingly.

Command Default

No rogue rules are configured.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

For your changes to be effective, you must enable the rule. You can configure up to 64 rules.

Reclassification of rogue APs according to the RSSI condition of the rogue rule occurs only when the RSSI changes more than +/- 2 dBm of the configured RSSI value. Manual and automatic classification override custom rogue rules. Rules are applied to manually changed rogues if their class type changes to unclassified and state changes to alert. Adhoc rogues are classified and do not go to the pending state. You can have up to 50 classification types.

The following example shows how to create a rule called rule_1 with a priority of 1 and a classification as friendly.

```
(Cisco Controller) > config rogue rule add ap priority 1 classify friendly rule_1
```

The following example shows how to enable rule_1.

```
(Cisco Controller) > config rogue rule enable rule_1
```

The following example shows how to change the priority of the last command.

```
(Cisco Controller) > config rogue rule priority 2 rule_1
```

The following example shows how to change the classification of the last command.

```
(Cisco Controller) > config rogue rule classify malicious rule_1
```

The following example shows how to disable the last command.

```
(Cisco Controller) > config rogue rule disable rule_1
```

The following example shows how to delete SSID_2 from the user-configured SSID list in rule-5.

```
(Cisco Controller) > config rogue rule condition ap delete ssid ssid_2 rule-5
```

The following example shows how to create a custom rogue rule.

```
(Cisco Controller) > config rogue rule classify custom 1 VeryMalicious rule6
```

Related Topics

config rogue adhoc, on page 380
config rogue auto-contain level
config rogue client, on page 390
config rogue containment
config rogue detection, on page 392
show rogue ignore-list, on page 338
show rogue rule detailed, on page 339
show rogue rule summary, on page 340
config rogue rule condition ap, on page 401

config rogue rule condition ap

To configure a condition of a rogue rule for rogue access points, use the **config rogue rule condition ap** command.

config rogue rule condition ap {**set** {**client-count** *count* | **duration** *time* | **managed-ssid** | **no-encryption** | **rssi** *rssi* | **ssid** *ssid* | **substring-ssid** *substring-ssid*} | **delete** {**all** | **client-count** | **duration** | **managed-ssid** | **no-encryption** | **rssi** | **ssid** | **substring-ssid**} *rule_name*

Syntax Description

set	Configures conditions to a rule that the rogue access point must meet.
client-count	Enables a minimum number of clients to be associated to the rogue access point.
count	Minimum number of clients to be associated to the rogue access point. The range is from 1 to 10 (inclusive). For example, if the number of clients associated to a rogue access point is greater than or equal to the configured value, the access point is classified as malicious.
duration	Enables a rogue access point to be detected for a minimum period of time.
time	Minimum time period, in seconds, to detect the rogue access point. The range is from 0 to 3600.
managed-ssid	Enables a rogue access point's SSID to be known to the controller.
no-encryption	Enables a rogue access point's advertised WLAN to not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it.
rssi	Enables a rogue access point to have a minimum Received Signal Strength Indicator (RSSI) value.

rssi	Minimum RSSI value, in dBm, required for the access point. The range is from –95 to –50 (inclusive). For example, if the rogue access point has an RSSI that is greater than the configured value, the access point is classified as malicious.
ssid	Enables a rogue access point have a specific SSID.
ssid	SSID of the rogue access point.
substring-ssid	Enables a rogue access point to have a substring of a user-configured SSID.
substring-ssid	Substring of a user-configured SSID. For example, if you have an SSID as ABCDE, you can specify the substring as ABCD or ABC. You can classify multiple SSIDs with matching patterns.
delete	Removes the conditions to a rule that a rogue access point must comply with.
all	Deletes all the rogue rule conditions.
rule_name	Rogue rule to which the command applies.

Command Default

The default value for RSSI is 0 dBm.

The default value for duration is 0 seconds.

The default value for client count is 0.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

You can configure up to 25 SSIDs per rogue rule. You can configure up to 25 SSID substrings per rogue rule.

The following example shows how to configure the RSSI rogue rule condition:

```
(Cisco Controller) > config rogue rule condition ap set rssi –50
```

config tacacs acct

To configure TACACS+ accounting server settings, use the **config tacacs acct** command.

config tacacs acct {**add***1-3 IP addr port ascii/hex secret* | **delete** *1-3* | **disable** *1-3* | **enable** *1-3* | **server-timeout** *1-3 seconds*}

Syntax Description

add	Adds a new TACACS+ accounting server.
1-3	Specifies TACACS+ accounting server index from 1 to 3.
IP addr	Specifies IPv4 or IPv6 address of the TACACS+ accounting server.
port	Specifies TACACS+ Server's TCP port.

ascii/hex	Specifies type of TACACS+ server's secret being used (ASCII or HEX).
secret	Specifies secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.
enable	Enables a TACACS+ server.
server-timeout	Changes the default server timeout for the TACACS+ server.
seconds	Specifies the number of seconds before the TACACS+ server times out. The server timeout range is from 5 to 30 seconds.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a new TACACS+ accounting server index 1 with the IPv4 address 10.0.0.0, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs acct add 1 10.0.0.0 10 ascii 12345678
```

The following example shows how to add a new TACACS+ accounting server index 1 with the IPv6 address 2001:9:6:40::623, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs acct add 1  2001:9:6:40::623 10 ascii 12345678
```

The following example shows how to configure the server timeout of 5 seconds for the TACACS+ accounting server:

```
(Cisco Controller) > config tacacs acct server-timeout 1 5
```

Related Topics

show tacacs acct statistics, on page 341
show tacacs summary, on page 343

config tacacs athr

To configure TACACS+ authorization server settings, use the **config tacacs athr** command.

config tacacs athr {**add***1-3 IP addr port ascii/hex secret* | **delete** *1-3* | **disable** *1-3* | **enable** *1-3* | **mgmt-server-timeout** *1-3 seconds* | **server-timeout** *1-3 seconds*}

Syntax Description

add	Adds a new TACACS+ authorization server (IPv4 or IPv6).
1-3	TACACS+ server index from 1 to 3.
IP addr	TACACS+ authorization server IP address (IPv4 or IPv6).
port	TACACS+ server TCP port.
ascii/hex	Type of secret key being used (ASCII or HEX).
secret	Secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.
enable	Enables a TACACS+ server.
mgmt-server-timeout *1-3seconds*	Changes the default management login server timeout for the server. The number of seconds before server times out is from 1 to 30 seconds.
server-timeout *1-3 seconds*	Changes the default network login server timeout for the server. The number of seconds before server times out is from 5 to 30 seconds.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a new TACACS+ authorization server index 1 with the IPv4 address 10.0.0.0, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs athr add 1 10.0.0.0 49 ascii 12345678
```

The following example shows how to add a new TACACS+ authorization server index 1 with the IPv6 address 2001:9:6:40::623, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs athr add 1 2001:9:6:40::623 49 ascii 12345678
```

The following example shows how to configure the retransmit timeout of 5 seconds for the TACACS+ authorization server:

```
(Cisco Controller) > config tacacs athr server-timeout 1 5
```

Related Topics

show tacacs athr statistics, on page 341

show tacacs summary, on page 343

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
```

Related Commands

config tacacs athr

config tacacs auth

To configure TACACS+ authentication server settings, use the **config tacacs auth** command.

config tacacs auth { **add***1-3 IP addr port ascii/hex secret* | **delete** *1-3* | **disable** *1-3* | **enable** *1-3* | **mgmt-server-timeout** *1-3 seconds* | **server-timeout** *1-3seconds* }

Syntax Description

add	Adds a new TACACS+ accounting server.
1-3	TACACS+ accounting server index from 1 to 3.
IP addr	IP address for the TACACS+ accounting server.
port	Controller port used for the TACACS+ accounting server.
ascii/hex	Type of secret key being used (ASCII or HEX).
secret	Secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.

enable	Enables a TACACS+ server.
mgmt-server-timeout *1-3 seconds*	Changes the default management login server timeout for the server. The number of seconds before server times out is from 1 to 30 seconds.
server-timeout *1-3 seconds*	Changes the default network login server timeout for the server. The number of seconds before server times out is from 5 to 30 seconds.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a new TACACS+ authentication server index 1 with the IPv4 address 10.0.0.3, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs auth add 1 10.0.0.3 49 ascii 12345678
```

The following example shows how to add a new TACACS+ authentication server index 1 with the IPv6 address 2001:9:6:40::623, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs auth add 1 2001:9:6:40::623 49 ascii 12345678
```

The following example shows how to configure the server timeout for TACACS+ authentication server:

```
(Cisco Controller) > config tacacs auth server-timeout 1 5
```

Related Topics

show tacacs auth statistics, on page 342
show tacacs summary, on page 343

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 tacacs dns

To retrieve the TACACS IP information from a DNS server, use the **config radius dns** command.

config radius dns { **global** *port* { *ascii* | *hex* } *secret* | **query** *url timeout* | **serverip** *ip_address* | **disable** | **enable** }

Syntax Description

global	Configures the global port and secret to retrieve the TACACS IP information from a DNS server.
port	Port number for authentication. The range is from 1 to 65535. All the DNS servers should use the same authentication port.
ascii	Format of the shared secret that you should set to ASCII.
hex	Format of the shared secret that you should set to hexadecimal.
secret	TACACS server login secret.
query	Configures the fully qualified domain name (FQDN) of the TACACS server and DNS timeout.
url	FQDN of the TACACS server. The FQDN can be up to 63 case-sensitive, alphanumeric characters.
timeout	Maximum time that the controller waits for, in days, before timing out a request and resending it. The range is from 1 to 180.
serverip	Configures the DNS server IP address.
ip_address	DNS server IP address.
disable	Disables the TACACS DNS feature. The default is disabled.
enable	Enables the controller to retrieve the TACACS IP information from a DNS server.

Command Default You cannot retrieve the TACACS IP information from a DNS server.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The accounting port is derived from the authentication port. All the DNS servers should use the same secret. When you enable a DNS query, the static configurations will be overridden. The DNS list overrides the static AAA list.

The following example shows how to enable the TACACS DNS feature on the controller:

```
(Cisco Controller) > config tacacs dns enable
```

Related Topics

config tacacs acct, on page 402
config tacacs athr, on page 403
config tacacs auth, on page 405
debug dns, on page 419

config tacacs fallback-test interval

To configure TACACS+ probing interval, use the **config tacacs fallback-test interval** command.

config tacacs fallback-test interval { *seconds* }

Syntax Description

seconds	TACACS+ probing interval in seconds. Disable is 0, Range from 180 to 3600 seconds.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure TACACS+ probing interval:

```
(Cisco Controller) > config tacacs fallback-test interval 200
```

config wlan radius_server realm

To configure realm on a WLAN, use the **config wlan radius_server realm** command.

config wlan *radius_server***realm** {**enable** | **disable**} *wlan-id*

Syntax Description

radius_server	Radius server index. The range is from 1 to 17.
enable	Enable realm on a WLAN.
disable	Disable realm on a WLAN.
wlan-id	WLAN ID. The range is from 1 to 512.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable realm on a WLAN:

```
(Cisco Controller) > config wlan 2 realm enable 50
```

config wlan security eap-params

To configure local EAP timers on a WLAN, use the **config wlan security eap-params** command.

config wlan security eap-params { {**enable** | **disbale**} | **eapol-key-timeout***timeout* | **eap-key-retries** *retries* | **identity-request-timeout** *timeout* | **identity-request-retries** *retries* | **request-timeout** *timeout* | **request-retries** *retries*} *wlan_id*

Syntax Description

{**enable** | **disable** }	Specifies to enable or disable SSID specific EAP timeouts or retries. The default value is disabled.
eapol-key-timeout *timeout*	Specifies the amount of time (200 to 5000 milliseconds) that the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The valid range is 200 to 5000 milliseconds. The default value is 1000 milliseconds.
eapol-key-retries *retries*	Specifies the maximum number of times (0 to 4 retries) that the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The default value is 2.
identity-request- timeout *timeout*	Specifies the amount of time (1 to 120 seconds) that the controller attempts to send an EAP identity request to wireless clients within WLAN using local EAP. The default value is 30 seconds.
identity-request-retries *retries*	Specifies the maximum number of times (0 to 4 retries) that the controller attempts to retransmit the EAP identity request to wireless clients within WLAN using local EAP. The default value is 2.

request-timeout	Specifies the amount of time (1 to 120 seconds) in which the controller attempts to send an EAP parameter request to wireless clients within WLAN using local EAP. The default value is 30 seconds.
request-retries*retries*	Specifies the maximum number of times (0 to 20 retries) that the controller attempts to retransmit the EAP parameter request to wireless clients within WLAN using local EAP. The default value is 2.
wlan-id	WLAN identification number.

Command Default

The default EAPOL key timeout is 1000 milliseconds.

The default for EAPOL key retries is 2.

The default identity request timeout is 30 seconds.

The default identity request retries is 2.

The default request timeout is 30 seconds.

The default request retries is 2.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable SSID specific EAP parameters on a WLAN:

```
(Cisco Controller) > config wlan security eap-params enable 4
```

The following example shows how to set EAPOL key timeout parameter on a WLAN:

```
(Cisco Controller) > config wlan security eap-params eapol-key-retries 4
```

The following example shows how to set EAPOL key retries on a WLAN:

```
(Cisco Controller) > config wlan security eap-params eapol-key-retries 4
```

clear Commands

This section lists the **clear** commands to clear existing security configurations of the controller.

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 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 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 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

debug Commands

This section lists the **debug** commands to manage debugging of security settings of the controller.

Caution Debug commands are reserved for use only under the direction of Cisco personnel. Do not use these commands without direction from Cisco-certified staff.

debug 11w-pmf

To configure the debugging of 802.11w, use the **debug 11w-pmf** command.

debug 11w-pmf {**all** | **events** | **keys**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all 802.11w messages.
keys	Configures the debugging of 802.11w keys.
events	Configures the debugging of 802.11w events.
enable	Enables the debugging of 802.1w options.
disable	Disables the debugging of 802.1w options.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging of 802.11w keys:

```
(Cisco Controller) >debug 11w-pmf keys enable
```

debug aaa

To configure the debugging of AAA settings, use the **debug aaa** command.

debug aaa {[**all** | **detail** | **events** | **packet** | **local-auth** | **tacacs**] [**enable** | **disable**]}

Syntax Description

all	(Optional) Configures the debugging of all AAA messages.
avp-xml	(Optional) Configures debug of AAA Avp xml events.
detail	(Optional) Configures the debugging of AAA errors.
events	(Optional) Configures the debugging of AAA events.

packet	(Optional) Configures the debugging of AAA packets.
local-auth	(Optional) Configures the debugging of the AAA local Extensible Authentication Protocol (EAP) events.
tacacs	(Optional) Configures the debugging of the AAA TACACS+ events.
enable	(Optional) Enables the debugging.
disable	(Optional) Disables the debugging.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.
8.6	The command is enhanced with new keyword. The new keyword is **avp-xml**.

Related Commands

debug aaa local-auth eap

show running-config

debug aaa events

To configure the debugging related to DNS-based ACLs, use the **debug aaa events enable** command.

debug aaa events enable

Syntax Description

events	Configures the debugging of DNS-based ACLs.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging for DNS-based ACLs:

```
(Cisco Controller) > debug aaa events enble
```

debug aaa local-auth

To configure the debugging of AAA local authentication on the controller, use the **debug aaa local-auth** command.

debug aaa local-auth { **db** | **shim** | **eap** { **framework** | **method** } { **all** | **errors** | **events** | **packets** | **sm** } } { **enable** | **disable** }

Syntax Description

db	Configures the debugging of the AAA local authentication back-end messages and events.
shim	Configures the debugging of the AAA local authentication shim layer events.
eap	Configures the debugging of the AAA local Extensible Authentication Protocol (EAP) authentication.
framework	Configures the debugging of the local EAP framework.
method	Configures the debugging of local EAP methods.
all	Configures the debugging of local EAP messages.
errors	Configures the debugging of local EAP errors.
events	Configures the debugging of local EAP events.
packets	Configures the debugging of local EAP packets.
sm	Configures the debugging of the local EAP state machine.
enable	Starts the debugging.
disable	Stops the debugging.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging of the AAA local EAP authentication:

```
(Cisco Controller) > debug aaa local-auth eap method all enable
```

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

show local-auth certificates

show local-auth config

show local-auth statistics

debug bcast

To configure the debugging of broadcast options, use the **debug bcast** command.

debug bcast {**all** | **error** | **message** | **igmp** | **detail**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all broadcast logs.
error	Configures the debugging of broadcast errors.
message	Configures the debugging of broadcast messages.
igmp	Configures the debugging of broadcast IGMP messages.
detail	Configures the debugging of broadcast detailed messages.
enable	Enables the broadcast debugging.
disable	Disables the broadcast debugging.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

```
(Cisco Controller) > debug bcast message enable
```

The following example shows how to disable the debugging of broadcast mesages:

```
(Cisco Controller) > debug bcast message disable
```

Related Commands

debug disable-all

show sysinfo

debug cckm

To configure the debugging of the Cisco Centralized Key Management options, use the **debug cckm**

debug cckm {**client** | **detailed**} {**enable** | **disable**}

Syntax Description

client	Configures debugging of the Cisco Centralized Key Management of clients.
detailed	Configures detailed debugging of Cisco Centralized Key Management.

enable	Enables debugging of Cisco Centralized Key Management.
disable	Disables debugging of Cisco Centralized Key Management.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable detailed debugging of Cisco Centralized Key Management:

```
(Cisco Controller) > debug cckm detailed enable
```

debug client

To configure the debugging for a specific client, use the **debug client** command.

debug client *mac_address*

Syntax Description

mac_address	MAC address of the client.

Command Default

None

Usage Guidelines

After entering the **debug client** *mac_address* command, if you enter the **debug aaa events enable** command, then the AAA events logs are displayed for that particular client MAC address.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to debug a specific client:

```
(Cisco Controller) > debug client 01:35:6x:yy:21:00
```

Related Topics

debug aaa events, on page 416

debug dns

To configure debugging of Domain Name System (DNS) options, use the **debug dns** command.

debug dns {**all** | **detail** | **error** | **message**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the DNS options.

detail	Configures debugging of the DNS details.
error	Configures debugging of the DNS errors.
message	Configures debugging of the DNS messages.
enable	Enables debugging of the DNS options.
disable	Disables debugging of the DNS options.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable DNS error debugging:

```
(Cisco Controller) > debug dns error enable
```

Related Topics

config radius dns, on page 378
config tacacs dns, on page 407

debug dot1x

To configure debugging of the 802.1X options, use the **debug dot1x** command.

debug dot1x {**aaa** | **all** | **events** | **packets** | **states**} {**enable** | **disable**}

Syntax Description

aaa	Configures debugging of the 802.1X AAA interactions.
all	Configures debugging of all the 802.1X messages.
events	Configures debugging of the 802.1X events.
packets	Configures debugging of the 802.1X packets.
states	Configures debugging of the 802.1X state transitions.
enable	Enables debugging of the 802.1X options.
disable	Disables debugging of the 802.1X options.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable 802.1X state transitions debugging:

```
(Cisco Controller) > debug dot1x states enable
```

Related Topics

config wlan security 802.1X, on page 483
config wlan security wpa akm 802.1x, on page 495

debug dtls

To configure debugging of the Datagram Transport Layer Security (DTLS) options, use the **debug dtls** command.

debug dtls {**all** | **event** | **packet** | **trace**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the DTLS messages.
event	Configures debugging of the DTLS events.
packet	Configures debugging of the DTLS packets.
trace	Configures debugging of the DTLS trace messages.
enable	Enables debugging of the DTLS options.
disable	Disables debugging of the DTLS options.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The debug actions described here are used in conjunction with CAPWAP troubleshooting.

The following example shows how to enable DTLS packet debugging:

```
(Cisco Controller) > debug dtls packet enable
```

Related Topics

show dtls connections, on page 25

debug pm

To configure the debugging of the security policy manager module, use the **debug pm** command.

debug pm {**all disable** | {**config** | **hwcrypto** | **ikemsg** | **init** | **list** | **message** | **pki** | **rng** | **rules** | **sa-export** | **sa-import** | **ssh-l2tp** | **ssh-appgw** | **ssh-engine** | **ssh-int** | **ssh-pmgr** | **ssh-ppp** | **ssh-tcp**} {**enable** | **disable**}}

Syntax Description

all disable	Disables all debugging in the policy manager module.

config	Configures the debugging of the policy manager configuration.
hwcrypto	Configures the debugging of hardware offload events.
ikemsg	Configures the debugging of Internet Key Exchange (IKE) messages.
init	Configures the debugging of policy manager initialization events.
list	Configures the debugging of policy manager list mgmt.
message	Configures the debugging of policy manager message queue events.
pki	Configures the debugging of Public Key Infrastructure (PKI) related events.
rng	Configures the debugging of random number generation.
rules	Configures the debugging of Layer 3 policy events.
sa-export	Configures the debugging of SA export (mobility).
sa-import	Configures the debugging of SA import (mobility).
ssh-l2tp	Configures the debugging of policy manager Layer 2 Tunneling Protocol (l2TP) handling.
ssh-appgw	Configures the debugging of application gateways.
ssh-engine	Configures the debugging of the policy manager engine.
ssh-int	Configures the debugging of the policy manager intercepter.
ssh-pmgr	Configures the debugging of the policy manager.
ssh-ppp	Configures the debugging of policy manager Point To Point Protocol (PPP) handling.
ssh-tcp	Configures the debugging of policy manager TCP handling.
enable	Enables the debugging.
disable	Disables the debugging.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the debugging of PKI-related events:

```
(Cisco Controller) > debug pm pki enable
```

Related Commands **debug disable-all**

debug web-auth

To configure debugging of web-authenticated clients, use the **debug web-auth** command.

debug web-auth {**redirect** { **enable mac** *mac_address* | **disable** } | **webportal-server** {**enable** | **disable** } }

Syntax Description

redirect	Configures debugging of web-authenticated and redirected clients.
enable	Enables the debugging of web-authenticated clients.
mac	Configures the MAC address of the web-authenticated client.
mac_address	MAC address of the web-authenticated client.
disable	Disables the debugging of web-authenticated clients.
webportal-server	Configures the debugging of portal authentication of clients.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging of a web authenticated and redirected client:

```
(Cisco Controller) > debug web-auth redirect enable mac xx:xx:xx:xx:xx:xx
```

WLAN Commands

show Commands

This section lists the **show** commands to display information about your WLAN configuration settings.

show advanced fra sensor

To display detailed information about the FRA configurations of the sensor, use the **show advanced fra sensor** command.

show advanced fra sensor

Syntax Description

advanced	Displays advanced configuration and statistics.
fra	Displays FRA configurations.
sensor	Displays FRA configurations for sensor

Command Default None

Command History

Release	Modification
8.5	This command was introduced.

The following example shows how to display information about the FRA sensor:

```
FRA State..................................... Enabled
FRA Operation State........................... Up
FRA Sensitivity............................... low (100%)
FRA Interval.................................. 1 Hour(s)
  Last Run.................................... 3563 seconds ago
  Last Run Time............................... 0 seconds
Service Priority.............................. Coverage


AP Name                          MAC Address       Slot Current Band   COF %      Sensor %
   Suggested Mode
------------------------------ ----------------- ---- -------------- ---------- ----------
 -------------------------
```

show client detail

To display detailed information for a client on a Cisco lightweight access point, use the **show client detail** command.

show client detail *mac_address*

Syntax Description

mac_address	Client MAC address.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The **show client ap** command may list the status of automatically disabled clients. Use the **show exclusionlist** command to display clients on the exclusion list.

The following example shows how to display the client detailed information:

```
(Cisco Controller) >show client detail 00:0c:41:07:33:a6
Policy Manager State.............................POSTURE_REQD
Policy Manager Rule Created.....................Yes
Client MAC Address.............................. 00:16:36:40:ac:58
Client Username................................. N/A
Client State.................................... Associated
Client NAC OOB State............................ QUARANTINE
Guest LAN Id.................................... 1
IP Address...................................... Unknown
Session Timeout................................. 0
QoS Level....................................... Platinum
802.1P Priority Tag............................. disabled
KTS CAC Capability.............................. Yes
WMM Support..................................... Enabled
Power Save...................................... ON
Diff Serv Code Point (DSPC)..................... disabled
Mobility State.................................. Local
Internal Mobility State......................... apfMsMmInitial
Security Policy Completed....................... No
Policy Manager State............................ WEBAUTH_REQD
Policy Manager Rule Created..................... Yes
NPU Fast Fast Notified.......................... Yes
Last Policy Manager State....................... WEBAUTH_REQD
Client Entry Create Time........................ 460 seconds
Interface....................................... wired-guest
FlexConnect Authentication...................... Local
FlexConnect Data Switching...................... Local
VLAN............................................ 236
Quarantine VLAN................................. 0
Client Statistics:
  Number of Bytes Received................... 66806
      Number of Data Bytes Received.................. 160783
      Number of Realtime Bytes Received.............. 160783
      Number of Data Bytes Sent...................... 23436
      Number of Realtime Bytes Sent.................. 23436
      Number of Data Packets Received................ 592
      Number of Realtime Packets Received............ 592
      Number of Data Packets Sent.................... 131
      Number of Realtime Packets Sent................ 131
      Number of Interim-Update Sent.............. 0
      Number of EAP Id Request Msg Timeouts...... 0
      Number of EAP Request Msg Timeouts......... 0
      Number of EAP Key Msg Timeouts............. 0
      Number of Data Retries..................... 0
      Number of RTS Retries...................... 0
      Number of Duplicate Received Packets....... 3
      Number of Decrypt Failed Packets........... 0
      Number of Mic Failured Packets............. 0
      Number of Mic Missing Packets.............. 0
  Number of RA Packets Dropped............... 6
      Number of Policy Errors.................... 0
```

```
      Radio Signal Strength Indicator..... -50 dBm
      Signal to Noise Ratio..... 43 dB
...
```

show client location-calibration summary

To display client location calibration summary information, use the **show client location-calibration summary** command.

show client location-calibration summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the location calibration summary information:

```
(Cisco Controller) >show client location-calibration summary
MAC Address Interval
----------- ----------
10:10:10:10:10:10 60
21:21:21:21:21:21 45
```

show client probing

To display the number of probing clients, use the **show client probing** command.

show client probing

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 number of probing clients:

```
(Cisco Controller) >show client probing
Number of Probing Clients..... 0
```

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.

Usage Guidelines

This command provides the following information:

- The time when the report was received
- The MAC address of the access point to which the client is currently associated
- The MAC address of the access point to which the client was previously associated
- The channel of the access point to which the client was previously associated
- The SSID of the access point to which the client was previously associated
- The time when the client disassociated from the previous access point
- The reason for the client roam

Note For non-CCXv4 clients, the Layer 2 roam reason is not displayed in the command output. For more information, see CSCvv85022.

Examples

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.

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 wlan

To display the summary of clients associated with a WLAN, use the **show client wlan** command.

show client wlan *wlan_id* [**devicetype** *device*]

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
devicetype	(Optional) Displays all clients with the specified device type.
device	Device type. For example, Samsung-Device or WindowsXP-Workstation.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following are sample outputs of the **show client wlan** command:

```
(Cisco Controller) > show client wlan 1

Number of Clients in WLAN..... 0


(Cisco Controller) > show client devicetype 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 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 icons file-info

To display icon parameters, use the **show icons file-info** command.

show icons file-info

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 sample output from the **show icons file-info** command:

```
Cisco Controller > show icons file-info

ICON File Info:
  No.   Filename                      Type         Lang  Width  Height
  ----  ------------------------      ------       ----  -----  ------
   1    dhk_icon.png                 png          eng   200    300
   2    myIconCopy2.png              png          eng   222    333
   3    myIconCopy1.png              png          eng   555    444
```

show network summary

To display the network configuration settings, 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.

The following example displays the output of the **show ipv6 summary** command:

```
(Cisco Controller) >show network summary
RF-Network Name.............................. johnny
Web Mode..................................... Enable
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 Forwarding................ Enable
Ethernet Broadcast Forwarding................ Enable
IPv4 AP Multicast/Broadcast Mode............. Multicast   Address : 239.9.9.9
IPv6 AP Multicast/Broadcast Mode............. Multicast   Address : ff1e::6:9
IGMP snooping................................ Enabled
IGMP timeout................................. 60 seconds
IGMP Query Interval.......................... 20 seconds
MLD snooping................................. Enabled
MLD timeout.................................. 60 seconds
MLD query interval........................... 20 seconds
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
Cisco AP Default Master...................... Disable
AP Join Priority............................. Disable
Mgmt Via Wireless Interface.................. Enable
Mgmt Via Dynamic Interface................... Enable
Bridge MAC filter Config..................... Enable
Bridge Security Mode......................... EAP
Mesh Full Sector DFS......................... Enable
AP Fallback ................................. Enable
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
Link Local Bridging Status .................. Disabled
CCX-lite status ............................. Disable
oeap-600 dual-rlan-ports .................... Disable
oeap-600 local-network ...................... Enable
oeap-600 Split Tunneling (Printers).......... Disable
WebPortal Online Client ..................... 0
WebPortal NTF_LOGOUT Client ................. 0
mDNS snooping................................ Disabled
mDNS Query Interval.......................... 15 minutes
Web Color Theme.............................. Default
L3 Prefer Mode............................... IPv4
```

show pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show pmk-cache** command.

show pmk-cache {**all** | *MAC*}

Syntax Description

all	Displays information about all entries in the PMK cache.
MAC	Information about a single entry in the PMK cache.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display information about a single entry in the PMK cache:

```
(Cisco Controller) >show pmk-cache xx:xx:xx:xx:xx:xx
```

The following example shows how to display information about all entries in the PMK cache:

```
(Cisco Controller) >show pmk-cache all
PMK Cache
                   Entry
Station            Lifetime   VLAN Override          IP Override
-----------------  --------   --------------------   ---------------
```

show rf-profile summary

To display a summary of RF profiles in the controller, use the **show rf-profile summary** command.

show rf-profile 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 the output of the **show rf-profile summary** command:

```
(Cisco Controller) >show rf-profile summary
Number of RF Profiles.......................... 2
Out Of Box State............................... Disabled
RF Profile Name            Band     Description                Applied
-------------------------  -------  -------------------------  -------
T1a                        5 GHz    <none>                     No
T1b                        2.4 GHz  <none>                     No
```

show rf-profile details

To display the RF profile details in the Cisco wireless LAN controller, use the **show rf-profile details** command.

show rf-profile details *rf-profile-name*

Syntax Description

rf-profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following is the output of the **show rf-profile details** command::

```
(Cisco Controller) >show rf-profile details T1a
Description..................................... <none>
Radio policy.................................... 5 GHz
Transmit Power Threshold v1..................... -70 dBm
Transmit Power Threshold v2..................... -67 dBm
Min Transmit Power.............................. -10 dBm
Max Transmit Power.............................. 30 dBm
Rx Sop Threshold................................ Medium
802.11a Operational Rates
    802.11a 6M Rate............................. Mandatory
    802.11a 9M Rate............................. Supported
    802.11a 12M Rate............................ Mandatory
    802.11a 18M Rate............................ Supported
    802.11a 24M Rate............................ Mandatory
    802.11a 36M Rate............................ Supported
    802.11a 48M Rate............................ Supported
    802.11a 54M Rate............................ Supported
Max Clients..................................... 200
Client Trap Threshold........................... 50
Multicast Data Rate............................. 0
Rx Sop Threshold................................ 0 dBm
Cca Threshold................................... 0 dBm
Slot Admin State:............................... Enabled
Band Select Probe Response...................... Disabled
Band Select Cycle Count......................... 2 cycles
Band Select Cycle Threshold..................... 200 milliseconds
Band Select Expire Suppression.................. 20 seconds
Band Select Expire Dual Band.................... 60 seconds
Band Select Client Rssi......................... -80 dBm
Load Balancing Denial........................... 3 count
Load Balancing Window........................... 5 clients
Coverage Data................................... -80 dBm
Coverage Voice.................................. -80 dBm
Coverage Exception.............................. 3 clients
Coverage Level.................................. 25 %
```

Related Topics

show rf-profile summary, on page 434
config rf-profile band-select, on page 445

show icons summary

To display a summary of the icons present in the flash memory of the system, use the **show icons summary** command.

show icons 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 sample output from the **show icons summary** command::

```
Cisco Controller > show icons summary

 Icon files (downloaded) in Flash memory
  No.   Filename                  Size
  ---  ----------------------    -----
    1.  dhk_icon.png                 120694
    2.  myIconCopy1.png              120694
    3.  myIconCopy2.png              120694
```

show wlan

To display configuration information for a specified wireless LAN or a foreign access point, or to display wireless LAN summary information, use the **show wlan** command.

show wlan { **apgroups** | **summary** | *wlan_id* | **foreignAp** | **lobby-admin-access**}

Syntax Description

apgroups	Displays access point group information.
summary	Displays a summary of all wireless LANs.
wlan_id	Displays the configuration of a WLAN. The Wireless LAN id to 512.
foreignAp	Displays the configuration for support of foreign access point

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 display a summary of wireless LANs for wlan_id 1:

```
(Cisco Controller) >show wlan 1
WLAN Identifier.................................. 1
Profile Name..................................... aicha
Network Name (SSID).............................. aicha
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Network Admission Control
   RADIUS Profiling Status ...................... Disabled
   DHCP ......................................... Disabled
   HTTP ......................................... Disabled
Client Profiling Status ...................... Disabled
   DHCP ......................................... Disabled
   HTTP ......................................... Disabled
   Radius-NAC State.............................. Enabled
   SNMP-NAC State................................ Enabled
Quarantine VLAN.................................. 0
Maximum number of Associated Clients............. 0
Maximum number of Clients per AP Radio........... 200
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
User Idle Timeout................................ 300 seconds
User Idle Threshold.............................. 0 Bytes
NAS-identifier................................... Talwar1
CHD per WLAN..................................... Enabled
Webauth DHCP exclusion........................... Disabled
Interface........................................ management
Multicast Interface.............................. Not Configured
WLAN IPv4 ACL.................................... unconfigured
WLAN IPv6 ACL.................................... unconfigured
mDNS Status...................................... Disabled
mDNS Profile Name................................ unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
```

```
Static IP client tunneling..... Enabled
PMIPv6 Mobility Type..... none
Quality of Service..... Silver (best effort)
Per-SSID Rate Limits..... Upstream      Downstream
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..... Upstream      Downstream
Average Data Rate.....   0              0
Average Realtime Data Rate.....   0              0
Burst Data Rate.....   0              0
Burst Realtime Data Rate.....   0              0
Scan Defer Priority..... 4,5,6
Scan Defer Time..... 100 milliseconds
WMM..... Allowed
WMM UAPSD Compliant Client Support..... Disabled
Media Stream Multicast-direct..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
Passive Client Feature..... Disabled
IPv6 Support..... Disabled
Peer-to-Peer Blocking Action..... Disabled
Radio Policy..... All
DTIM period for 802.11a radio..... 1
DTIM period for 802.11b radio..... 1
Radius Servers
   Authentication..... Global Servers
   Accounting..... Global Servers
   Interim Update..... Disabled
   Dynamic Interface..... Disabled
Local EAP Authentication..... Enabled (Profile 'Controller_Local_EAP')
Radius NAI-Realm..... Enabled
Security
   802.11 Authentication:..... Open System
    FT Support..... Disabled
   Static WEP Keys..... Disabled
   802.1X..... Disabled
   Wi-Fi Protected Access (WPA/WPA2)..... Enabled
      WPA (SSN IE)..... Enabled
         TKIP Cipher..... Disabled
         AES Cipher..... Enabled
      WPA2 (RSN IE)..... Enabled
         TKIP Cipher..... Disabled
         AES Cipher..... Enabled
Auth Key Management
         802.1x..... Enabled
         PSK..... Disabled
         CCKM..... Enabled
         FT(802.11r)..... Disabled
         FT-PSK(802.11r)..... Disabled
         PMF-1X(802.11w)..... Enabled
         PMF-PSK(802.11w)..... Disabled
FT Reassociation Timeout..... 20
FT Over-The-Air mode..... Enabled
FT Over-The-Ds mode..... Enabled
      GTK Randomization..... Disabled
      SKC Cache Support..... Disabled
      CCKM TSF Tolerance..... 1000
   Wi-Fi Direct policy configured..... Disabled
   EAP-Passthrough..... Disabled
```

```
CKIP ..................................... Disabled
   IP Security.................................. Disabled
   IP Security Passthru......................... Disabled
   Web Based Authentication..................... Disabled
   Web-Passthrough.............................. Disabled
   Conditional Web Redirect..................... Disabled
   Splash-Page Web Redirect..................... Disabled
   Auto Anchor.................................. Disabled
   FlexConnect Local Switching.................. Enabled
   flexconnect Central Dhcp Flag................ Disabled
   flexconnect nat-pat Flag..................... Disabled
   flexconnect Dns Override Flag................ Disabled
   FlexConnect Vlan based Central Switching ..... Disabled
   FlexConnect Local Authentication............. Disabled
   FlexConnect Learn IP Address................. Enabled
   Client MFP................................... Optional
   PMF.......................................... Disabled
   PMF Association Comeback Time................ 1
   PMF SA Query RetryTimeout.................... 200
   Tkip MIC Countermeasure Hold-down Timer..... 60
Call Snooping................................... Disabled
Roamed Call Re-Anchor Policy.................... Disabled
SIP CAC Fail Send-486-Busy Policy............... Enabled
SIP CAC Fail Send Dis-Association Policy........ Disabled
KTS based CAC Policy............................ Disabled
Band Select..................................... Disabled
Load Balancing.................................. Disabled
 Mobility Anchor List
 WLAN ID     IP Address            Status
 -------     ---------------       ------
802.11u..................................... Enabled
  Network Access type.......................... Chargeable Public Network
  Internet service............................. Enabled
  Network Authentication type.................. Not Applicable
  HESSID....................................... 00:00:00:00:00:00
  IP Address Type Configuration
    IPv4 Address type.........................  Available
    IPv6 Address type.........................  Not Known

  Roaming Consortium List
    Index       OUI List     In Beacon
    -----   --------------   ---------
      1         313131       Yes
      2         DDBBCC       No
      3         DDDDDD       Yes
 Realm configuration summary
    Realm index.................................. 1
    Realm name................................... jobin
      EAP index.................................. 1
      EAP method................................. Unsupported
    Index   Inner Authentication           Authentication Method
    -----   --------------------           ---------------------
        1                Credential Type                    SIM
        2   Tunneled Eap Credential Type                    SIM
        3                Credential Type                    SIM
        4                Credential Type                   USIM
        5                Credential Type         Hardware Token
        6                Credential Type              SoftToken
  Domain name configuration summary
    Index  Domain name
    -------------------
        1   rom3
        2   ram
        3   rom1
```

```
Hotspot 2.0..................................... Enabled

  Operator name configuration summary
    Index   Language   Operator name
    -----   --------   -------------
        1        ros   Robin

  Port config summary
 Index   IP protocol   Port number   Status
    -----   -----------   -----------   -------
        1             1             0    Closed
        2             1             0    Closed
        3             1             0    Closed
        4             1             0    Closed
        5             1             0    Closed
        6             1             0    Closed
        7             1             0    Closed
 WAN Metrics Info
    Link status.................................. Up
    Symmetric Link............................... No
    Downlink speed............................... 4 kbps
    Uplink speed................................. 4 kbps

MSAP Services................................... Disabled
Local Policy
----------------
Priority  Policy Name
--------  ---------------
   1        Teacher_access_policy
```

The following example shows how to display a summary of all WLANs:

```
(Cisco Controller) >show wlan summary
Number of WLANs................................. 1

WLAN ID  WLAN Profile Name / SSID               Status    Interface Name        PMIPv6
Mobility
-------  -------------------------------------  --------  --------------------
---------------
1        apsso / apsso                          Disabled  management            none
```

The following example shows how to display the configuration for support of foreign access points:

```
(Cisco Controller) >show wlan foreignap
Foreign AP support is not enabled.
```

The following example shows how to display the AP groups:

```
(Cisco Controller) >show wlan apgroups
Total Number of AP Groups....................... 1
Site Name....................................... APuser
Site Description................................ <none>
Venue Name...................................... Not configured
Venue Group Code.................................Unspecified
Venue Type Code..................................Unspecified
Language Code................................... Not configured
AP Operating Class.............................. 83,84,112,113,115,116,117,118,123
RF Profile
----------
```

```
2.4 GHz band..................................... <none>
5 GHz band....................................... <none>
WLAN ID          Interface          Network Admission Control          Radio Policy
-------          -----------        --------------------------         ------------
 14              int_4                Disabled                          All
AP Name             Slots  AP Model             Ethernet MAC       Location          Port
 Country  Priority
------------------  -----  -------------------  -----------------  ----------------  ----
 -------  --------
Ibiza                2     AIR-CAP2602I-A-K9    44:2b:03:9a:8a:73  default location  1
 US       1
Larch                2     AIR-CAP3502E-A-K9    f8:66:f2:ab:23:95  default location  1
 US       1

Zest                 2     AIR-CAP3502I-A-K9    00:22:90:91:6d:b6               ren  1
 US       1

Number of Clients................................ 1

MAC Address       AP Name          Status        Device Type
----------------- ---------- ------------ -----------------

24:77:03:89:9b:f8      ap2       Associated      Android
```

config Commands

This section lists the **config** commands to configure WLANs.

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 advanced apgroup-global-ntp

To configure a global NTP server for AP groups, use the **config advanced apgroup-global-ntp** command.

config advanced apgroup-global-ntp add *server-index*{**enable** | **disable**}
config advanced apgroup-global-ntp delete

Syntax Description

add	Allows you to add an index for the AP group global NTP server.
ntp-server-index	Allows you to configure the NTP server index.
enable	Enables the authentication for the AP group global NTP server.
disable	Disables the authentication for the AP group global NTP server.
delete	Deletes the AP group global NTP server.

Command History

Release	Modification
8.10	This command was introduced.

The following example shows how to enable a global NTP server (with an index value of 3):

```
(Cisco Controller) > config advanced apgroup-global-ntp add 3 enable
```

config advanced fra interval

To auto-configure voice deployment in WLANs, use the **config auto-configure voice** command.

config advanced fra interval *value*

Syntax Description

advanced	Advanced configuration.
fra	To configure FRA parameters.
interval	To configure FRA interval in hours.
value	Value of the FRA interval in house.

Command Default None

Command History

Release	Modification
8.5	This command was introduced.

config client deauthenticate

To disconnect a client, use the **config client deauthenticate** command.

config client deauthenticate {*MAC* | *IPv4/v6_address* | *user_name*}

Syntax Description

MAC	Client MAC address.
IPv4/v6_address	IPv4 or IPv6 address.
user_name	Client user name.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to deauthenticate a client using its MAC address:

```
(Cisco Controller) >config client deauthenticate 11:11:11:11:11:11
```

config client profiling delete

To delete client profile , use the **config client profiling** command.

config client profiling delete { *mac_address* }

Syntax Description

mac_address	MAC address of the client.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to delete a client profile:

```
(Cisco Controller) >config client profiling delete 37:15:86:2a:Bc:cf
```

Note Executing the above command changes the Device Type to "Unknown". The Client does not get deleted but instead the profiling info of the client is removed, and retains the client as it is still associated. There is no confirmation message from the CLI, due to architecture limitation of the controller.

config icons delete

To delete an icon or icons from flash, use the **config icons delete** command in the WLAN configuration mode.

config icons delete { *filename* | **all** }

Syntax Description

filename	Name of the icon to be deleted.
all	Deletes all the icon files from the system.

Command Default None

Command Modes WLAN configuration

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to delete an icon from flash:

```
Cisco Controller > config icons delete image-1
```

config icons file-info

To configure an icon parameter, use the **config icons file-info** command in WLAN configuration mode.

config icons file-info *filename file-type lang-code width height*

Syntax Description

filename	Icon filename. It can be up to 32 characters long.
file-type	Icon filename type or extension. It can be up to 32 characters long.
lang-code	Language code of the icon. Enter 2 or 3 letters from ISO-639, for example: *eng* for English.
width	Icon width. The range is from 1 to 65535.
height	Icon height. The range is from 1 to 65535.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to configure icon parameters:

```
Cisco Controller > config icons file-info ima png eng 300 200
```

config rf-profile band-select

To configure the RF profile band selection parameters, use the **config rf-profile band-select** command.

config rf-profile band-select {**client-rssi** *rssi* | **cycle-count** *cycles* | **cycle-threshold** *value* | **expire** {**dual-band** *value* | **suppression** *value*} | **probe-response** {**enable** | **disable**}} *profile_name*

Syntax Description

client-rssi	Configures the client Received Signal Strength Indicator (RSSI) threshold for the RF profile.
rssi	Minimum RSSI for a client to respond to a probe. The range is from -20 to -90 dBm.
cycle-count	Configures the probe cycle count for the RF profile. The cycle count sets the number of suppression cycles for a new client.
cycles	Value of the cycle count. The range is from 1 to 10.
cycle-threshold	Configures the time threshold for a new scanning RF Profile band select cycle period. This setting determines the time threshold during which new probe requests from a client come in a new scanning cycle.
value	Value of the cycle threshold for the RF profile. The range is from 1 to 1000 milliseconds.

expire	Configures the expiration time of clients for band select.
dual-band	Configures the expiration time for pruning previously known dual-band clients. After this time elapses, clients become new and are subject to probe response suppression.
value	Value for a dual band. The range is from 10 to 300 seconds.
suppression	Configures the expiration time for pruning previously known 802.11b/g clients. After this time elapses, clients become new and are subject to probe response suppression.
value	Value for suppression. The range is from 10 to 200 seconds.
probe-response	Configures the probe response for a RF profile.
enable	Enables probe response suppression on clients operating in the 2.4-GHz band for a RF profile.
disable	Disables probe response suppression on clients operating in the 2.4-GHz band for a RF profile.
profile name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

The default value for client RSSI is –80 dBm.

The default cycle count is 2.

The default cycle threshold is 200 milliseconds.

The default value for dual-band expiration is 60 seconds.

The default value for suppression expiration is 20 seconds.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4-GHz and moves the dual band clients to the 5-Ghz spectrum. The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.

The following example shows how to configure the client RSSI:

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

config rf-profile channel

To configure the RF profile DCA settings, use the **config rf-profile channel** command.

config rf-profile channel {**add** *chan profile name* | **delete** *chan profile name* | **foreign** {**enable** | **disable**} *profile name* | **chan-width** {**20** | **40** | **80**} *profile name*}

Syntax Description

add	Adds channel to the RF profile DCA channel list.
delete	Removes channel from the RF profile DCA channel list.
foreign	Configures the RF profile DCA foreign AP contribution.
chan-width	Configures the RF profile DCA channel width.
chan	Specifies channel number.
profile name	Specifies the name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
enable	Enables foreign AP interference.
disable	Disables foreign AP interference.
{**20** | **40** | **80**}	Specifies RF Profile DCA channel width.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a channel to the RF profile DCA channel list:

```
(Cisco Controller) >config rf-profile channel add 40 admin1
```

The following example shows how to configure the RF profile DCA channel width:

```
(Cisco Controller) >config rf-profile channel chan-width 40 admin1
```

config rf-profile client-trap-threshold

To configure the threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller, use the **config rf-profile client-trap-threshold** command.

config rf-profile client-trap-threshold *threshold profile_name*

Syntax Description

threshold	Threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller. The range is from 0 to 200. Traps are disabled if the threshold value is configured as zero.
profile_name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

None

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 an access point:

```
(Cisco Controller) >config rf-profile client-trap-threshold 150
```

config rf-profile create

To create a RF profile, use the **config rf-profile create** command.

config rf-profile create {**802.11a** | **802.11b/g**} *profile-name*

Syntax Description

802.11a	Configures the RF profile for the 2.4GHz band.
802.11b/g	Configures the RF profile for the 5GHz band.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

```
(Cisco Controller) >config rf-profile create 802.11a RFtestgroup1
```

config rf-profile fra client-aware

To configure the RF profile client-aware FRA feature, use the **config rf-profile fra client-aware** command.

config rf-profile fra client-aware {**client-reset** *percent rf-profile-name* | **client-select** *percent rf-profile-name* | **disable** *rf-profile-name* | **enable** *rf-profile-name*}

Syntax Description

client-reset	Configures the RF profile AP utilization threshold for radio to switch back to Monitor mode.
percent	Utilization percentage value ranges from 0 to 100. The default is 5%.
rf-profile-name	Name of the RF Profile.
client-select	Configures the RF profile utilization threshold for radio to switch to 5GHz.
percent	Utilization percentage value ranges from 0 to 100. The default is 50%.
disable	Disables the RF profile client-aware FRA feature.
enable	Enables the RF profile client-aware FRA feature.

Command Default

The default percent value for client-select and client-reset is 50% and 5% respectively.

Command History

Release	Modification
8.5	This command was introduced.

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch back from 5GHz client-serving role to Monitor mode:

```
(Cisco Controller) >config rf-profile fra client-aware client-reset 15 profile1
```

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch from Monitor mode to 5GHz client-serving role:

```
(Cisco Controller) >config rf-profile fra client-aware client-select 20 profile1
```

The following example shows how to disable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware disable profile1
```

The following example shows how to enable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware enable profile1
```

config rf-profile data-rates

To configure the data rate on a RF profile, use the **config rf-profile data-rates** command.

config rf-profile data-rates {**802.11a** | **802.11b** } {**disabled** | **mandatory** | **supported**} *data-rate profile-name*

Syntax Description

802.11a	Specifies 802.11a as the radio policy of the RF profile.
802.11b	Specifies 802.11b as the radio policy of the RF profile.
disabled	Disables a rate.
mandatory	Sets a rate to mandatory.
supported	Sets a rate to supported.
data-rate	802.11 operational rates, which are 1*, 2*, 5.5*, 6, 9, 11*, 12, 18, 24, 36, 48 and 54, where * denotes 802.11b only rates.
profile-name	Name of the RF profile.

Command Default

Default data rates for RF profiles are derived from the controller system defaults, the global data rate configurations. For example, if the RF profile's radio policy is mapped to 802.11a then the global 802.11a data rates are copied into the RF profiles at the time of creation.

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 of an RF profile at a mandatory rate at 12 Mbps:

```
(Cisco Controller) >config rf-profile 802.11b data-rates mandatory 12 RFGroup1
```

config rf-profile delete

To delete a RF profile, use the **config rf-profile delete** command.

config rf-profile delete *profile-name*

Syntax Description

profile-name	Name of the RF profile.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to delete a RF profile:

```
(Cisco Controller) >config rf-profile delete RFGroup1
```

config rf-profile description

To provide a description to a RF profile, use the **config rf-profile description** command.

config rf-profile description *description profile-name*

Syntax Description

description	Description of the RF profile.
profile-name	Name of the RF profile.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a description to a RF profile:

```
(Cisco Controller) >config rf-profile description This is a demo desciption RFGroup1
```

config rf-profile load-balancing

To configure load balancing on an RF profile, use the **config rf-profile load-balancing** command.

config rf-profile load-balancing {**window** *clients* | **denial** *value*} *profile_name*

Syntax Description

window	Configures the client window for load balancing of an RF profile.
clients	Client window size that limits the number of client associations with an access point. The range is from 0 to 20. The default value is 5. The window size is part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations: *load-balancing window + client associations on AP with lightest load = load-balancing threshold* Access points with more client associations than this threshold are considered busy, and clients can associate only to access points with client counts lower than the threshold. This window also helps to disassociate sticky clients.
denial	Configures the client denial count for load balancing of an RF profile.
value	Maximum number of association denials during load balancing. The range is from 1 to 10. The default value is 3. When a client tries to associate on a wireless network, it sends an association request to the access point. If the access point is overloaded and load balancing is enabled on the controller, the access point sends a denial to the association request. If there are no other access points in the range of the client, the client tries to associate the same access point again. After the maximum denial count is reached, the client is able to associate. Association attempts on an access point from any client before associating any AP is called a sequence of association. The default is 3.
profile_name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the client window size for an RF profile:

```
(Cisco Controller) >config rf-profile load-balancing window 15
```

config rf-profile max-clients

To configure the maximum number of client connections per access point of an RF profile, use the **config rf-profile max-clients** commands.

config rf-profile max-clients *clients*

Syntax Description

clients	Maximum number of client connections per access point of an RF profile. The range is from 1 to 200.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

You can use this command to configure the maximum number of clients on access points that are in client dense areas, or serving high bandwidth video or mission critical voice applications.

The following example shows how to set the maximum number of clients at 50:

```
(Cisco Controller) >config rf-profile max-clients 50
```

config rf-profile multicast data-rate

To configure the minimum RF profile multicast data rate, use the **config rf-profile multicast data-rate** command.

config rf-profile multicast data-rate *value profile_name*

Syntax Description

value	Minimum RF profile multicast data rate. The options are 6, 9, 12, 18, 24, 36, 48, 54. Enter 0 to specify that access points will dynamically adjust the data rate.
profile_name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

The minimum RF profile multicast data rate is 0.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to set the multicast data rate for an RF profile:

```
(Cisco Controller) >config rf-profile multicast data-rate 24
```

config rf-profile out-of-box

To create an out-of-box AP group consisting of newly installed access points, use the **config rf-profile out-of-box** command.

config rf-profile out-of-box {**enable** | **disable**}

Syntax Description

enable	Enables the creation of an out-of-box AP group. When you enable this command, the following occurs: • Newly installed access points that are part of the default AP group will be part of the out-of-box AP group and their radios will be switched off, which eliminates any RF instability caused by the new access points. • All access points that do not have a group name become part of the out-of-box AP group. • Special RF profiles are created per 802.11 band. These RF profiles have default-settings for all the existing RF parameters and additional new configurations.
disable	Disables the out-of-box AP group. When you disable this feature, only the subscription of new APs to the out-of-box AP group stops. All APs that are subscribed to the out-of-box AP group remain in this AP group. You can move APs to the default group or a custom AP group upon network convergence.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When an out-of-box AP associates with the controller for the first time, it will be redirected to a special AP group and the RF profiles applicable to this AP Group will control the radio admin state configuration of the AP. You can move APs to the default group or a custom group upon network convergence.

The following example shows how to enable the creation of an out-of-box AP group:

```
(Cisco Controller) >config rf-profile out-of-box enable
```

config rf-profile rx-sop threshold

To configure high, medium or low Rx SOP threshold values for each 802.11 band, use the **config rf-profile rx-sop threshold** command.

config rf-profile rx-sop threshold {**high** | **medium** | **low** | **auto**} *profile_name*

Syntax Description

high	Configures the high Rx SOP threshold value for an RF profile.
medium	Configures the medium Rx SOP threshold value for an RF profile.
low	Configures the low Rx SOP threshold value for an RF profile.

auto	Configures an auto Rx SOP threshold value for an RF profile. When you choose auto, the access point determines the best Rx SOP threshold value.
profile_name	RF profile on which the Rx SOP threshold value will be configured.

Command Default

The default Rx SOP threshold option is auto.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the high Rx SOP threshold value on an RF profile:

```
(Cisco Controller) > config 802.11 rx-sop threshold high T1a
```

Related Topics

config 802.11 rx-sop threshold, on page 703
show 802.11 extended, on page 674

config rf-profile trap-threshold

To configure the RF profile trap threshold, use the **config rf-profile trap-threshold** command.

config rf-profile trap-threshold {**clients** *clients profile name* | **interference** *percent profile name* | **noise** *dBm profile name* | **utilization** *percent profile name*}

Syntax Description

clients	Configures the RF profile trap threshold for clients.
clients	The number of clients on an access point's radio for the trap is between 1 and 200. The default is 12 clients.
profile name	Specifies the name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
interference	Configures the RF profile trap threshold for interference.
percent	The percentage of interference threshold for the trap is from 0 to 100 %. The default is 10 %.
noise	Configures the RF profile trap threshold for noise.
dBM	The level of noise threshold for the trap is from -127 to 0 dBm. The default is -17 dBm.
utilization	Configures the RF profile trap threshold for utilization.
percent	The percentage of bandwidth being used by an access point threshold for the trap is from 0 to 100 %. The default is 80 %.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the RF profile trap threshold for clients:

```
(Cisco Controller) >config rf-profile trap-threshold clients 50 admin1
```

config rf-profile tx-power-control-thresh-v1

To configure Transmit Power Control version1 (TPCv1) to an RF profile, use the **config rf-profile tx-power-control-thresh-v1** command.

config rf-profile tx-power-control-thresh-v1 *tpc-threshold profile_name*

Syntax Description

tpc-threshold	TPC threshold.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure TPCv1 on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v1 RFGroup1
```

config rf-profile tx-power-control-thresh-v2

To configure Transmit Power Control version 2 (TPCv2) to an RF profile, use the **config rf-profile tx-power-control-thresh-v2** command.

config rf-profile tx-power-control-thresh-v2 *tpc-threshold profile-name*

Syntax Description

tpc-threshold	TPC threshold.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure TPCv2 on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v2 RFGroup1
```

config rf-profile tx-power-max

To configure maximum auto-rf to an RF profile, use the **config rf-profile tx-power-max** command.

config rf-profile *tx-power-max profile-name*

Syntax Description

tx-power-max	Maximum auto-rf tx power.
profile-name	Name of the RF profile.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure tx-power-max on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-max RFGroup1
```

config rf-profile tx-power-min

To configure minimum auto-rf to an RF profile, use the **config rf-profile tx-power-min** command.

config rf-profile tx-power-min *tx-power-min profile-name*

Syntax Description

tx-power-min	Minimum auto-rf tx power.
profile-name	Name of the RF profile.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure tx-power-min on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-min RFGroup1
```

config time apgroup ntp

To configure an NTP server for an AP group, use the **config time apgroup ntp** command.

config time apgroup ntp auth {**enable** *server-index key-index* | **disable** *server-index*}
config time apgroup ntp delete *server-index*
config time apgroup ntp key-auth { {**add** *key-index* {**md5** | **sha1**} {**ascii** | **hex**} *key* } | | {**delete** *key-index*} }

config time apgroup ntp server *server-index ip-address*

Syntax Description

config time apgroup ntp auth	
auth	Configures NTP authentication.
enable	Enables NTP authentication.
server-index	NTP server index.
key-index	Key index. Valid range is from 1 to 65535.
disable	Disables NTP authentication.
config time apgroup ntp delete	
delete	Deletes a per-AP group NTP server. **Note** You cannot delete a per-AP group NTP server if it is being used by an AP group.
config time apgroup ntp key-auth	
key-auth	Configures an NTP authentication key.
add	Enables you to add an NTP authentication key.
delete	Enables you to delete an NTP authentication key.
key-index	Key index. Valid range is from 1 to 65535.
md5 |**sha1**	Key type to choose from. The default key type is MD5.
ascii |**hex**	Key format to choose from. The default value is ASCII.
key	Key value. • For MD5, the maximum characters for the key is 16. • For SHA1, the maximum characters for the key is 20.
config time apgroup ntp server	
server	Configures NTP server.
ip-address	IP address of the server. Both IPv4 and IPv6 adrdress formats are supported.

Command Default

None

Command History

Release	Modification
8.10	This command was introduced.

The following example shows you how to configure a per-AP group NTP server whose server index is 2 and the IPv4 address is 209.165.200.230:

```
(Cisco Controller) > config time apgroup ntp server 2 209.165.200.230
```

The following example shows you how to configure an NTP key for authentication for AP groups with MD5 as the checksum and ASCII as the key format:

```
(Cisco Controller) > config time apgroup ntp key-auth add 3 md5 ascii example123
```

config watchlist add

To add a watchlist entry for a wireless LAN, use the **config watchlist add** command.

config watchlist add {**mac** *MAC* | **username** *username*}

Syntax Description

mac *MAC*	Specifies the MAC address of the wireless LAN.
username *username*	Specifies the name of the user to watch.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a watchlist entry for the MAC address a5:6b:ac:10:01:6b:

```
(Cisco Controller) >config watchlist add mac a5:6b:ac:10:01:6b
```

config watchlist delete

To delete a watchlist entry for a wireless LAN, use the **config watchlist delete** command.

config watchlist delete {**mac** *MAC* | **username** *username*}

Syntax Description

mac *MAC*	Specifies the MAC address of the wireless LAN to delete from the list.
username *username*	Specifies the name of the user to delete from the list.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to delete a watchlist entry for the MAC address a5:6b:ac:10:01:6b:

```
(Cisco Controller) >config watchlist delete mac a5:6b:ac:10:01:6b
```

config watchlist disable

To disable the client watchlist, use the **config watchlist disable** command.

config watchlist disable

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 disable the client watchlist:

```
(Cisco Controller) >config watchlist disable
```

config watchlist enable

To enable a watchlist entry for a wireless LAN, use the **config watchlist enable** command.

config watchlist enable

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 enable a watchlist entry:

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

config wlan

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

config wlan {**enable** | **disable** | **create** | **delete**} *wlan_id* [*name* | **foreignAp** *name ssid* | **all**]

Syntax Description

enable	Enables a wireless LAN.

disable	Disables a wireless LAN.
create	Creates a wireless LAN.
delete	Deletes a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.
name	(Optional) WLAN profile name up to 32 alphanumeric characters.
foreignAp	(Optional) Specifies the third-party access point settings.
ssid	SSID (network name) up to 32 alphanumeric characters.
all	(Optional) Specifies all wireless LANs.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When you create a new WLAN using the **config wlan create** command, it is created in disabled mode. Leave it disabled until you have finished configuring it.

If you do not specify an SSID, the profile *name* parameter is used for both the profile name and the SSID.

If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

The following example shows how to enable wireless LAN identifier 16:

```
(Cisco Controller) >config wlan enable 16
```

config wlan 7920-support

To configure support for phones, use the **config wlan 7920-support** command.

config wlan 7920-support {**client-cac-limit** | **ap-cac-limit**} {**enable** | **disable**} *wlan_id*

Syntax Description

ap-cac-limit	Supports phones that require client-controlled Call Admission Control (CAC) that expect the Cisco vendor-specific information element (IE).
client-cac-limit	Supports phones that require access point-controlled CAC that expect the IEEE 802.11e Draft 6 QBSS-load.

enable	Enables phone support.
disable	Disables phone support.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

The following example shows how to enable the phone support that requires client-controlled CAC with wireless LAN ID 8:

```
(Cisco Controller) >config wlan 7920-support ap-cac-limit enable 8
```

config wlan 802.11e

To configure 802.11e support on a wireless LAN, use the **config wlan 802.11e** command.

config wlan 802.11e {**allow** | **disable** | **require**} *wlan_id*

Syntax Description

allow	Allows 802.11e-enabled clients on the wireless LAN.
disable	Disables 802.11e on the wireless LAN.
require	Requires 802.11e-enabled clients on the wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

802.11e provides quality of service (QoS) support for LAN applications, which are critical for delay sensitive applications such as Voice over Wireless IP (VoWIP).

802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability and is especially well suited for use in networks that include a multimedia capability.

The following example shows how to allow 802.11e on the wireless LAN with LAN ID 1:

```
(Cisco Controller) >config wlan 802.11e allow 1
```

config wlan aaa-override

To configure a user policy override via AAA on a wireless LAN, use the **config wlan aaa-override** command.

config wlan aaa-override {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

enable	Enables a policy override.
disable	Disables a policy override.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

AAA is disabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When AAA override is enabled and a client has conflicting AAA and Cisco wireless LAN controller wireless LAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system will move clients from the default Cisco wireless LAN VLAN to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system will also use QoS, DSCP, 802.1p priority tag values, and ACLs provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as Identity Networking.)

If the corporate wireless LAN uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.

When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is performed by the AAA server if the controller wireless LAN does not contain any client-specific authentication parameters.

The AAA override values might come from a RADIUS server.

The following example shows how to configure user policy override via AAA on WLAN ID 1:

```
(Cisco Controller) >config wlan aaa-override enable 1
```

config wlan apgroup ntp

To configure NTP authentication for an AP group and map the NTP server to the AP group, use the **config wlan apgroup ntp** command.

config wlan apgroup ntp add *ap-group-name server-index*
config wlan apgroup ntp auth *ap-group-name* {**enable** | **disable**}
config wlan apgroup ntp delete *ap-group-name*

Syntax Description

add	Enables you to add an NTP server to an AP group.
ap-group-name server-index	Name of the AP group that you want to configure.
server-index	Index value of the NTP server
auth	Option to enable or disable NTP authentication for the AP group.
enable	Enables NTP authentication for the AP group.
disable	Disables NTP authentication for the AP group.
delete	Option to delete NTP server.

Command History

Release	Modification
8.10	This command was introduced.

The following example shows you how to add an AP group named test123 with a server index value of 3:

```
(Cisco Controller) > config wlan apgroup ntp test123 3
```

config wlan assisted-roaming

To configure assisted roaming on a WLAN, use the **config wlan assisted-roaming** command.

config wlan assisted-roaming {**neighbor-list** | **dual-list** | **prediction**} {**enable** | **disable**} *wlan_id*

Syntax Description

neighbor-list	Configures an 802.11k neighbor list for a WLAN.
dual-list	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
prediction	Configures an assisted roaming optimization prediction for a WLAN.
enable	Enables the configuration on the WLAN.
disable	Disables the configuration on the WLAN.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

The 802.11k neighbor list is enabled for all WLANs.

By default, dual band list is enabled if the neighbor list feature is enabled for the WLAN.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN, if load balancing is already enabled on the WLAN.

The following example shows how to enable an 802.11k neighbor list for a WLAN:

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```

config wlan band-select allow

To configure band selection on a WLAN, use the **config wlan band-select allow** command.

config wlan band-select allow {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables band selection on a WLAN.
disable	Disables band selection on a WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines When you enable band select on a WLAN, the access point suppresses client probes on 2.4-GHz and moves the dual band clients to the 5-Ghz spectrum. The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.

The following example shows how to enable band selection on a WLAN:

```
(Cisco Controller) >config wlan band-select allow enable 6
```

config wlan broadcast-ssid

To configure an Service Set Identifier (SSID) broadcast on a wireless LAN, use the **config wlan broadcast-ssid** command.

config wlan broadcast-ssid {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables SSID broadcasts on a wireless LAN.
disable	Disables SSID broadcasts on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default Broadcasting of SSID is disabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure an SSID broadcast on wireless LAN ID 1:

```
(Cisco Controller) >config wlan broadcast-ssid enable 1
```

config wlan chd

To enable or disable Coverage Hole Detection (CHD) for a wireless LAN, use the **config wlan chd** command.

config wlan chd *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables SSID broadcasts on a wireless LAN.
disable	Disables SSID broadcasts on a wireless LAN.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable CHD for WLAN 3:

```
(Cisco Controller) >config wlan chd 3 enable
```

config wlan ccx aironet-ie

To enable or disable Aironet information elements (IEs) for a WLAN, use the **config wlan ccx aironet-ie** command.

config wlan ccx aironet-ie {**enable** | **disable**}

Syntax Description

enable	Enables the Aironet information elements.
disable	Disables the Aironet information elements.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable Aironet information elements for a WLAN:

```
(Cisco Controller) >config wlan ccx aironet-ie enable
```

config wlan channel-scan defer-priority

To configure the controller to defer priority markings for packets that can defer off channel scanning, use the **config wlan channel-scan defer-priority** command.

config wlan channel-scan defer-priority *priority* [**enable** | **disable**] *wlan_id*

Syntax Description

priority	User priority value (0 to 7).
enable	(Optional) Enables packet at given priority to defer off channel scanning.
disable	(Optional) Disables packet at gven priority to defer off channel scanning.
wlan_id	Wireless LAN identifier (1 to 512).

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The priority value should be set to 6 on the client and on the WLAN.

The following example shows how to enable the controller to defer priority markings that can defer off channel scanning with user priority value 6 and WLAN id 30:

```
(Cisco Controller) >config wlan channel-scan defer-priority 6 enable 30
```

config wlan channel-scan defer-time

To assign the channel scan defer time in milliseconds, use the **config wlan channel-scan defer-time** command.

config wlan channel-scan defer-time *msecs wlan_id*

Syntax Description

msecs	Deferral time in milliseconds (0 to 60000 milliseconds).
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The time value in milliseconds should match the requirements of the equipment on your WLAN.

The following example shows how to assign the scan defer time to 40 milliseconds for WLAN with ID 50:

```
(Cisco Controller) >config wlan channel-scan defer-time 40 50
```

config wlan custom-web

To configure the web authentication page for a WLAN, use the **config wlan custom-web** command.

config wlan custom-web { { **ext-webauth-url** *ext-webauth-url wlan_id* } | { **global** { **enable** | **disable** } } | { **ms-open** { **enable** | **disable** | **url** } } | { **login-page** *page-name* } | { **loginfailure-page** { *page-name* | **none** } } | { **logout-page** { *page-name* | **none** } } | { **sleep-client** { **enable** | **disable** } *wlan_id* **timeout** *duration* } | { **webauth-type** { **internal** | **customized** | **external** } *wlan_id* } }

Syntax Description

ext-webauth-url	Configures an external web authentication URL.
ext-webauth-url	External web authentication URL.
wlan_id	WLAN identifier. Default range is from 1 to 512.
global	Configures the global status for a WLAN.
enable	Enables the global status for a WLAN.
disable	Disables the global status for a WLAN.
ms-open	Configures the ms-open feature on the WLAN.
enable	Enables the ms-open feature on the WLAN.
disable	Disables the ms-open feature on the WLAN.
url	Configures ms-open URL.
login-page	Configures the name of the login page for an external web authentication URL.
page-name	Login page name for an external web authentication URL.
loginfailure-page	Configures the name of the login failure page for an external web authentication URL.
none	Does not configure a login failure page for an external web authentication URL.
logout-page	Configures the name of the logout page for an external web authentication URL.
sleep-client	Configures the sleep client feature on the WLAN.
timeout	Configures the sleep client timeout on the WLAN.

duration	Maximum amount of time after the idle timeout, in hours, before a sleeping client is forced to reauthenticate. The range is from 1 to 720. The default is 12. When the sleep client feature is enabled, the clients need not provide the login credentials when they move from one controller to another (if the controllers are in the same mobility group) between the sleep and wake-up times.
webauth-type	Configures the type of web authentication for the WLAN.
internal	Displays the default login page.
customized	Displays a customized login page.
external	Displays a login page on an external web server.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure web authentication type in the WLAN.

```
Cisco Controller config wlan custom-web webauth-type external
```

config wlan dtim

To configure a Delivery Traffic Indicator Message (DTIM) for 802.11 radio network **config wlan dtim** command.

config wlan dtim {**802.11a** | **802.11b**} *dtim wlan_id*

Syntax Description

802.11a	Configures DTIM for the 802.11a radio network.
802.11b	Configures DTIM for the 802.11b radio network.
dtim	Value for DTIM (between 1 to 255 inclusive).
wlan_id	Number of the WLAN to be configured.

Command Default

The default is DTIM 1.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure DTIM for 802.11a radio network with DTIM value 128 and WLAN ID 1:

```
(Cisco Controller) >config wlan dtim 802.11a 128 1
```

config wlan exclusionlist

To configure the wireless LAN exclusion list, use the **config wlan exclusionlist** command.

config wlan exclusionlist {*wlan_id* [**enabled** | **disabled** | *time*] | **foreignAp** [**enabled** | **disabled** | *time*]}

Syntax Description

wlan_id	Wireless LAN identifier (1 to 512).
enabled	(Optional) Enables the exclusion list for the specified wireless LAN or foreign access point.
disabled	(Optional) Disables the exclusion list for the specified wireless LAN or a foreign access point.
time	(Optional) Exclusion list timeout in seconds. A value of zero (0) specifies infinite time.
foreignAp	Specifies a third-party access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

This command replaces the **config wlan blacklist** command.

The following example shows how to enable the exclusion list for WLAN ID 1:

```
(Cisco Controller) >config wlan exclusionlist 1 enabled
```

config wlan flexconnect central-assoc

To configure client reassociation and security key caching on the controller, use the **config wlan flexconnect central-assoc** command.

config wlan flexconnect central-assoc *wlan-id* { **enable** | **disable** }

Syntax Description

wlan-id	ID of the WLAN
enable	Enables client reassociation and security key caching on the controller
disable	Disables client reassociation and security key caching on the controller

Command Default Client reassociation and security key caching on the controller is in the disabled state.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines A use case for this configuration is a large-scale deployment with fast roaming.

Configuration of central association with local authentication is not supported for the WLAN. After the PMIPv6 tunnel is set up, all data traffic from the PMIPv6 clients are forwarded from the Cisco AP to the local mobility anchor (LMA) in the Generic Routing Encapsulation (GRE) tunnel. If the connectivity between the Cisco AP and the controller is lost, the data traffic for the existing PMIPv6 clients continues to flow until the connectivity between the Cisco AP and the client is lost. When the AP is in stand-alone mode, no new client associations are accepted on the PMIPv6-enabled WLAN.

The following example shows how to enable client reassociation and security key caching on the controller for a WLAN whose ID is 2:

```
(Cisco Controller) >config wlan flexconnect central-assoc 2 enable
```

config wlan flexconnect learn-ipaddr

To enable or disable client IP address learning for the Cisco WLAN controller, use the **config wlan flexconnect learn-ipaddr** command.

config wlan flexconnect learn-ipaddr *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables client IPv4 address learning on a wireless LAN.
disable	Disables client IPv4 address learning on a wireless LAN.

Command Default Disabled when the **config wlan flexconnect local-switching** command is disabled. Enabled when the **config wlan flexconnect local-switching** command is enabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines If the client is configured with Layer 2 encryption, the controller cannot learn the client IP address, and the controller will periodically drop the client. Disable this option to keep the client connection without waiting to learn the client IP address.

Note This command is valid only for IPv4.

Note The ability to disable IP address learning is not supported with FlexConnect central switching.

The following example shows how to disable client IP address learning for WLAN 6:

```
(Cisco Controller) >config wlan flexconnect learn-ipaddr disable 6
```

Related Commands **show wlan**

config wlan flexconnect local-switching

To configure local switching, central DHCP, NAT-PAT, or the override DNS option on a FlexConnect WLAN, use the **config wlan flexconnect local switching** command.

config wlan flexconnect local-switching *wlan_id* {**enable** | **disable**} { {**central-dhcp** {**enable** | **disable**} **nat-pat** {**enable** | **disable**} } | {**override option dns** { **enable** | **disable**} } }

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
enable	Enables local switching on a FlexConnect WLAN.
disable	Disables local switching on a FlexConnect WLAN.
central-dhcp	Configures central switching of DHCP packets on the local s When you enable this feature, the DHCP packets received fr to the controller and forwarded to the corresponding VLAN
enable	Enables central DHCP on a FlexConnect WLAN.
disable	Disables central DHCP on a FlexConnect WLAN.
nat-pat	Configures Network Address Translation (NAT) and Port Ad local switching FlexConnect WLAN.
enable	Enables NAT-PAT on the FlexConnect WLAN.
disable	Disables NAT-PAT on the FlexConnect WLAN.
override	Specifies the DHCP override options on the FlexConnect W
option dns	Specifies the override DNS option on the FlexConnect WLA the clients get their DNS server IP address from the AP, not f
enable	Enables the override DNS option on the FlexConnect WLAN
disable	Disables the override DNS option on the FlexConnect WLA

Command Default This feature is disabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When you enable the **config wlan flexconnect local-switching** command, the **config wlan flexconnect learn-ipaddr** command is enabled by default.

Note This command is valid only for IPv4.

Note The ability to disable IP address learning is not supported with FlexConnect central switching.

The following example shows how to enable WLAN 6 for local switching and enable central DHCP and NAT-PAT:

```
(Cisco Controller) >config wlan flexconnect local-switching 6 enable central-dhcp enable
nat-pat enable
```

The following example shows how to enable the override DNS option on WLAN 6:

```
(Cisco Controller) >config wlan flexconnect local-switching 6 override option dns enable
```

config wlan flexconnect sae anti-clog-threshold

To configure Simultaneous Authentication of Equals (SAE) anticlog threshold in a FlexConnect deployment, use the **config wlan flexconnect sae anti-clog-threshold** command.

config wlan flexconnect sae anti-clog-threshold *limit*

Syntax Description

limit	Anticlogging enable threshold limit in terms of SAE block in a FlexConnect deployment. Valid range is 0 to 90.

Command Default

None

Command History

Release	Modification
8.10	This command was introduced.

Usage Guidelines

If the anticlogging threshold limit is 90, anticlogging is enforced by the controller when the number of clients reaches 90 percent of the supported number.

The following example shows how to configure 10 as the anticlogging threshold limit in a FlexConnect deployment:

```
(Cisco Controller) > config wlan flexconnect sae anti-clog-threshold 10
```

config wlan flexconnect sae max-retry

To configure the maximum number of retries for a Simultaneous Authentication of Equals (SAE) message in a FlexConnect deployment, use the **config wlan flexconnect sae max-retry** command.

config wlan flexconnect sae max-retry *limit*

Syntax Description

limit	Maximum number of retransmission attempts for an SAE message in a FlexConnect deployment. Valid range is 2 to 4.

Command Default

None

Command History

Release	Modification
8.10	This command was introduced.

The following example shows how to configure 4 as the maximum number of retries for an SAE message in a FlexConnect deployment:

```
(Cisco Controller) > config wlan flexconnect sae max-retry 4
```

config wlan flexconnect sae retry-timeout

To configure timeout period for an SAE message in a FlexConnect deployment, use the **config wlan flexconnect sae retry-timeout** command.

config wlan flexconnect sae retry-timeout *timeout*

Syntax Description

timeout	SAE message retry timeout in a FlexConnect deployment. Valid range is 200 to 2000 milliseconds.

Command Default

None

Command History

Release	Modification
8.10	This command was introduced.

The following example shows how to configure timeout period in a FlexConnect deployment for an SAE message to 400 milliseconds:

```
(Cisco Controller) > config wlan flexconnect sae retry-timeout 400
```

config wlan interface

To configure a wireless LAN interface or an interface group, use the **config wlan interface** command.

config wlan interface {*wlan_id* | **foreignAp**} {*interface-name* | *interface-group-name*}

Syntax Description

wlan_id	(Optional) Wireless LAN identifier (1 to 512).
foreignAp	Specifies third-party access points.
interface-name	Interface name.
interface-group-name	Interface group name.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure an interface named VLAN901:

```
(Cisco Controller) >config wlan interface 16 VLAN901
```

config wlan kts-cac

To configure the Key Telephone System-based CAC policy for a WLAN, use the **config wlan kts-cac** command.

config wlan kts-cac {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the KTS-based CAC policy.
disable	Disables the KTS-based CAC policy.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines To enable the KTS-based CAC policy for a WLAN, ensure that you do the following:

- Configure the QoS profile for the WLAN to Platinum by entering the following command:

  config wlan qos *wlan-id* **platinum**
- Disable the WLAN by entering the following command:

  config wlan disable *wlan-id*
- Disable FlexConnect local switching for the WLAN by entering the following command:

  config wlan flexconnect local-switching *wlan-id* **disable**

The following example shows how to enable the KTS-based CAC policy for a WLAN with the ID 4:

```
(Cisco Controller) >config wlan kts-cac enable 4
```

config wlan load-balance

To override the global load balance configuration and enable or disable load balancing on a particular WLAN, use the **config wlan load-balance** command.

config wlan load-balance allow {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables band selection on a wireless LAN.
disable	Disables band selection on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Load balancing is enabled by default.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable band selection on a wireless LAN with WLAN ID 3:

```
(Cisco Controller) >config wlan load-balance allow enable 3
```

config wlan max-associated-clients

To configure the maximum number of client connections on a wireless LAN, guest LAN, or remote LAN, use the **config wlan max-associated-clients** command.

config wlan max-associated-clients *max_clients wlan_id*

Syntax Description

max_clients	Maximum number of client connections to be accepted.
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 specify the maximum number of client connections on WLAN ID 2:

```
(Cisco Controller) >config wlan max-associated-clients 25 2
```

config wlan max-radio-clients

To configure the maximum number of WLAN client per access point, use the **config wlan max-radio-clients** command.

config wlan max-radio-clients *max_radio_clients wlan_id*

Syntax Description

max_radio_clients	Maximum number of client connections to be accepted per access point radio. The valid range is from 1 to 200.
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 specify the maximum number of client connections per access point radio on WLAN ID 2:

```
(Cisco Controller) >config wlan max-radio-clients 25 2
```

config wlan media-stream

To configure multicast-direct for a wireless LAN media stream, use the **config wlan media-stream** command.

config wlan media-stream multicast-direct {*wlan_id* | **all**} {**enable** | **disable**}

Syntax Description

multicast-direct	Configures multicast-direct for a wireless LAN media stream.
wlan_id	Wireless LAN identifier between 1 and 512.
all	Configures the wireless LAN on all media streams.
enable	Enables global multicast to unicast conversion.
disable	Disables global multicast to unicast conversion.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines Media stream multicast-direct requires load based Call Admission Control (CAC) to run. WLAN quality of service (QoS) needs to be set to either gold or platinum.

The following example shows how to enable the global multicast-direct media stream with WLAN ID 2:

```
(Cisco Controller) >config wlan media-stream multicast-direct 2 enable
```

config wlan mu-mimo

To enable Multi-User, Multiple-Input, Multiple-Output (MU-MIMO) on a WLAN, enter the **config wlan mu-mimo** command.

config wlan mu-mimo {**enable** | **disable**} *wlan-id*

Syntax Description

enable *wlan-id*	Enables MU-MIMO on the WLAN that is specified
disable *wlan-id*	Disables MU-MIMO on the WLAN that is specified

Command History

Release	Modification
8.3	This command was introduced.

config wlan nac radius

To configure RADIUS Network Admission Control (NAC) out-of-band support for a WLAN, use the **config wlan nac radius** command.

config wlan nac radius { **enable** | **disable** } *wlan_id*

Syntax Description

enable	Enables RADIUS NAC out-of-band support for a WLAN
disable	Disables RADIUS NAC out-of-band support for a WLAN
wlan_id	WLAN identifier. Valid range is between 1 and 512.

Command Default None

Command History

Release	Modification
8.7	This command was introduced.

Examples The following example shows how to enable RADIUS NAC out-of-band support for WLAN ID 34:

```
(Cisco Controller) >config wlan nac radius enable 34
```

config wlan pmipv6 default-realm

To configure a default realm for a PMIPv6 WLAN, use the **config wlan pmipv6 default-realm** command.

config wlan pmipv6 default-realm { *default-realm-name* | **none** } *wlan_id*

Syntax Description

default-realm-name	Default realm name for the WLAN.
none	Clears the realm name for the WLAN.
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 a default realm name on a PMIPv6 WLAN:

```
(Cisco Controller) >config wlan pmipv6 default-realm XYZ 6
```

config wlan profile

To edit a profile associated to a WLAN, use the **config wlan profile** command.

config wlan profile *wlan_id profile-name*

Syntax Description

wlan_id	WLAN identifier from 1 to 512.
profile-name	Name of the WLAN profile.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to edit a profile associated to a WLAN:

```
(Cisco Controller) > config wlan disable 1
(Cisco Controller) > config wlan profile 1 new_sample
(Cisco Controller) > show wlan summary

Number of WLANs.............................. 1

WLAN ID  WLAN Profile Name / SSID    Status    Interface Name    PMIPv6 Mobility
-------  -------------------------   --------  ---------------   ---------------
1        new_sample / new_samp       Disabled  management            none
```

config wlan profiling

To configure client profiling on a WLAN, use the **config wlan profiling** command.

config wlan profiling { **local** | **radius** } { **all** | **dhcp** | **http** } { **enable** | **disable** } *wlan_id*

Syntax Description

local	Configures client profiling in Local mode for a WLAN.
radius	Configures client profiling in RADIUS mode on a WLAN.
all	Configures DHCP and HTTP client profiling in a WLAN.
dhcp	Configures DHCP client profiling alone in a WLAN.
http	Configures HTTP client profiling in a WLAN.
enable	Enables the specific type of client profiling in a WLAN. When you enable HTTP profiling, the controller collects the HTTP attributes of clients for profiling. When you enable DHCP profiling, the controller collects the DHCP attributes of clients for profiling.
disable	Disables the specific type of client profiling in a WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.

Usage Guidelines

Ensure that you have disabled the WLAN before configuring client profiling on the WLAN.

Command Default

Client profiling is disabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Only clients connected to port 80 for HTTP can be profiled. IPv6 only clients are not profiled.

If a session timeout is configured for a WLAN, clients must send the HTTP traffic before the configured timeout to get profiled.

This feature is not supported on the following:

- FlexConnect Standalone mode
- FlexConnect Local Authentication

The following example shows how to enable both DHCP and HTTP profiling on a WLAN:

```
(Cisco Controller) >config wlan profiling radius all enable 6
                                        HTTP Profiling successfully enabled.
                                        DHCP Profiling successfully enabled.
```

config wlan qos

To change the quality of service (QoS) for a wireless LAN, use the **config wlan qos** command.

config wlan qos *wlan_id* {**bronze** | **silver** | **gold** | **platinum**}
config wlan qos foreignAp {**bronze** | **silver** | **gold** | **platinum**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
bronze	Specifies the bronze QoS policy.
silver	Specifies the silver QoS policy.
gold	Specifies the gold QoS policy.
platinum	Specifies the platinum QoS policy.
foreignAp	Specifies third-party access points.

Command Default

The default QoS policy is silver.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to set the highest level of service on wireless LAN 1:

```
(Cisco Controller) >config wlan qos 1 gold
```

config wlan radio

To set the Cisco radio policy on a wireless LAN, use the **config wlan radio** command.

config wlan radio *wlan_id* {**all** | **802.11a** | **802.11bg** | **802.11g** | **802.11ag**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
all	Configures the wireless LAN on all radio bands.
802.11a	Configures the wireless LAN on only 802.11a.
802.11bg	Configures the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled).
802.11g	Configures the wireless LAN on 802.11g only.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the wireless LAN on all radio bands:

```
(Cisco Controller) >config wlan radio 1 all
```

config wlan radius_server acct

To configure RADIUS accounting servers of a WLAN, use the **config wlan radius_server acct** command.

config wlan radius_server acct {**enable** | **disable**} *wlan_id* | **add** *wlan_id server_id* | **delete** *wlan_id* {**all** | *server_id*} | **framed-ipv6** { **address** | **both** | **prefix** } *wlan_id*}

Syntax Description

enable	Enables RADIUS accounting for the WLAN.
disable	Disables RADIUS accounting for the WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.
add	Adds a link to a configured RADIUS accounting server.
server_id	RADIUS server index.
delete	Deletes a link to a configured RADIUS accounting server.
address	Configures an accounting framed IPv6 attribute to an IPv6 address.
both	Configures the accounting framed IPv6 attribute to an IPv6 address and prefix.
prefix	Configures the accounting framed IPv6 attribute to an IPv6 prefix.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable RADIUS accounting for the WLAN 2:

```
(Cisco Controller) >config wlan radius_server acct enable 2
```

The following example shows how to add a link to a configured RADIUS accounting server:

```
(Cisco Controller) > config wlan radius_server acct add 2 5
```

config wlan radius_server acct interim-update

To configure the interim update of a RADIUS accounting server of a WLAN, use the **config wlan radius_server acct interim-update** command.

config wlan radius_server acct interim-update {**enable** | **disable** | *interval* } *wlan_id*

Syntax Description

interim-update	Configures the interim update of the RADIUS accounting server.
enable	Enables interim update of the RADIUS accounting server for the WLAN.
disable	Disables interim update of the RADIUS accounting server for the WLAN.
interval	Interim update interval that you specify. The valid range is 180 seconds to 3600 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Interim update of a RADIUS accounting sever is set at 600 seconds.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to specify an interim update of 200 seconds to a RADIUS accounting server of WLAN 2:

```
(Cisco Controller) >config wlan radius_server acct interim-update 200 2
```

config wlan radius_server auth

To configure RADIUS authentication servers of a WLAN, use the **config wlan radius_server auth** command.

config wlan radius_server auth {**enable** *wlan_id* | **disable** *wlan_id*} {**add** *wlan_id server_id* | **delete** *wlan_id* {**all** | *server_id*}}

Syntax Description

auth	Configures a RADIUS authentication
enable	Enables RADIUS authentication for this WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.
disable	Disables RADIUS authentication for this WLAN.
add	Adds a link to a configured RADIUS server.
server_id	RADIUS server index.
delete	Deletes a link to a configured RADIUS server.
all	Deletes all links to configured RADIUS servers.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a link to a configured RADIUS authentication server with WLAN ID 1 and Server ID 1:

```
(Cisco Controller) >config wlan radius_server auth add 1 1
```

config wlan radius_server acct interim-update

To configure the interim update of a RADIUS accounting server of a WLAN, use the **config wlan radius_server acct interim-update** command.

config wlan radius_server acct interim-update {**enable** | **disable** | *interval* } *wlan_id*

Syntax Description

interim-update	Configures the interim update of the RADIUS accounting server.
enable	Enables interim update of the RADIUS accounting server for the WLAN.
disable	Disables interim update of the RADIUS accounting server for the WLAN.
interval	Interim update interval that you specify. The valid range is 180 seconds to 3600 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default Interim update of a RADIUS accounting sever is set at 600 seconds.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to specify an interim update of 200 seconds to a RADIUS accounting server of WLAN 2:

```
(Cisco Controller) >config wlan radius_server acct interim-update 200 2
```

config wlan security 802.1X

To change the state of 802.1X security on the wireless LAN Cisco radios, use the **config wlan security 802.1X** command.

config wlan security 802.1X {**enable** {*wlan_id* | **foreignAp**} | **disable** {*wlan_id* | **foreignAp**} | **encryption** {*wlan_id* | **foreignAp**} {**0** | **40** | **104**} | **on-macfilter-failure** {**enable** | **disable**}}

Syntax Description

enable	Enables the 802.1X settings.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
disable	Disables the 802.1X settings.
encryption	Specifies the static WEP keys and indexes.
0	Specifies a WEP key size of 0 (no encryption) bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
40	Specifies a WEP key size of 40 bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
104	Specifies a WEP key size of 104 bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
on-macfilter-failure	Configures 802.1X on MAC filter failure.
enable	Enables 802.1X authentication on MAC filter failure.
disable	Disables 802.1X authentication on MAC filter failure.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

To change the encryption level of 802.1X security on the wireless LAN Cisco radios, use the following key sizes:

- 0—no 802.1X encryption.
- 40—40/64-bit encryption.
- 104—104/128-bit encryption. (This is the default encryption setting.)

The following example shows how to configure 802.1X security on WLAN ID 16.

```
(Cisco Controller) >config wlan security 802.1X enable 16
```

config wlan security ckip

To configure Cisco Key Integrity Protocol (CKIP) security options for the wireless LAN, use the **config wlan security ckip** command.

config wlan security ckip {**enable** | **disable**} *wlan_id* [**akm psk set-key** {**hex** | **ascii**} {**40** | **104**} **key** *key_index wlan_id* | **mmh-mic** {**enable** | **disable**} *wlan_id* | **kp** {**enable** | **disable**} *wlan_id*]

Syntax Description

enable	Enables CKIP security.
disable	Disables CKIP security.
wlan_id	Wireless LAN identifier from 1 to 512.
akm psk set-key	(Optional) Configures encryption key management for the CKIP wireless LAN.
hex	Specifies a hexadecimal encryption key.
ascii	Specifies an ASCII encryption key.
40	Sets the static encryption key length to 40 bits for the CKIP WLAN. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters.
104	Sets the static encryption key length to 104 bits for the CKIP WLAN. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.
key	Specifies the CKIP WLAN key settings.
key_index	Configured PSK key index.
mmh-mic	(Optional) Configures multi-modular hash message integrity check (MMH MIC) validation for the CKIP wireless LAN.
kp	(Optional) Configures key-permutation for the CKIP wireless LAN.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure a CKIP WLAN encryption key of 104 bits (26 hexadecimal characters) for PSK key index 2 on WLAN 03:

```
(Cisco Controller) >config wlan security ckip akm psk set-key hex 104 key 2 03
```

config wlan security cond-web-redir

To enable or disable conditional web redirect, use the **config wlan security cond-web-redir** command.

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables conditional web redirect.
disable	Disables conditional web redirect.
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 enable the conditional web direct on WLAN ID 2:

```
(Cisco Controller) >config wlan security cond-web-redir enable 2
```

config wlan security eap-passthru

To configure the 802.1X frames pass through on to the external authenticator, use the **config wlan security eap-passthru** command.

config wlan security eap-passthru {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables 802.1X frames pass through to external authenticator.
disable	Disables 802.1X frames pass through to external authenticator.
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 enable the 802.1X frames pass through to external authenticator on WLAN ID 2:

```
(Cisco Controller) >config wlan security eap-passthru enable 2
```

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
```

config wlan security ft over-the-ds

To configure 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** command.

config wlan security ft over-the-ds {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables 802.11r fast transition roaming support over a distributed system.
disable	Disables 802.11r fast transition roaming support over a distributed system.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Enabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

Ensure that 802.11r fast transition is enabled on the WLAN.

The following example shows how to enable 802.11r fast transition roaming support over a distributed system on WLAN ID 2:

```
(Cisco Controller) >config wlan security ft over-the-ds enable 2
```

config wlan security passthru

To modify the IPsec pass-through used on the wireless LAN, use the **config wlan security passthru** command.

config wlan security passthru {**enable** | **disable**} {*wlan_id* | **foreignAp**} [*ip_address*]

Syntax Description

enable	Enables IPsec pass-through.
disable	Disables IPsec pass-through.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
ip_address	(Optional) IP address of the IPsec gateway (router) that is terminating the VPN tunnel.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to modify IPsec pass-through used on the wireless LAN:

```
(Cisco Controller) >config wlan security passthru enable 3 192.12.1.1
```

config wlan security splash-page-web-redir

To enable or disable splash page web redirect, use the **config wlan security splash-page-web-redir** command.

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables splash page web redirect.
disable	Disables splash page web redirect.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default Splash page web redirect is disabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable spash page web redirect:

```
(Cisco Controller) >config wlan security splash-page-web-redir enable 2
```

config wlan security static-wep-key authentication

To configure static Wired Equivalent Privacy (WEP) key 802.11 authentication on a wireless LAN, use the **config wlan security static-wep-key authentication** command.

config wlan security static-wep-key authentication {**shared-key** | **open**} *wlan_id*

Syntax Description

shared-key	Enables shared key authentication.
open	Enables open system authentication.
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 enable the static WEP shared key authentication for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key authentication shared-key 1
```

config wlan security static-wep-key disable

To disable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key disable** command.

config wlan security static-wep-key disable *wlan_id*

Syntax Description

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 disable the static WEP keys for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key disable 1
```

config wlan security static-wep-key enable

To enable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key enable** command.

config wlan security static-wep-key enable *wlan_id*

Syntax Description

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 enable the use of static WEK keys for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key enable 1
```

config wlan security static-wep-key encryption

To configure the static Wired Equivalent Privacy (WEP) keys and indexes, use the **config wlan security static-wep-key encryption** command.

config wlan security static-wep-key encryption *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key key-index*

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
40	Specifies the encryption level of 40.
104	Specifies the encryption level of 104.
hex	Specifies to use hexadecimal characters to enter key.
ascii	Specifies whether to use ASCII characters to enter key.
key	WEP key in ASCII.
key-index	Key index (1 to 4).

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

One unique WEP key index can be applied to each wireless LAN. Because there are only four WEP key indexes, only four wireless LANs can be configured for static WEP Layer 2 encryption.

Make sure to disable 802.1X before using this command.

The following example shows how to configure the static WEP keys for WLAN ID 1 that uses hexadecimal character 0201702001 and key index 2:

```
(Cisco Controller) >config wlan security static-wep-key encryption 1 40 hex 0201702001 2
```

config wlan security tkip

To configure the Temporal Key Integrity Protocol (TKIP) Message Integrity Check (MIC) countermeasure hold-down timer, use the **config wlan security tkip** command.

config wlan security tkip hold-down *time wlan_id*

Syntax Description

hold-down	Configures the TKIP MIC countermeasure hold-down timer.
time	TKIP MIC countermeasure hold-down time in seconds. The range is from 0 to 60 seconds.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

The default TKIP countermeasure is set to 60 seconds.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

TKIP countermeasure mode can occur if the access point receives 2 MIC errors within a 60 second period. When this situation occurs, the access point deauthenticates all TKIP clients that are associated to that 802.11 radio and holds off any clients for the countermeasure holdoff time.

The following example shows how to configure the TKIP MIC countermeasure hold-down timer:

```
(Cisco Controller) >config wlan security tkip
```

config wlan security web-auth

To change the status of web authentication used on a wireless LAN, use the **config wlan security web-auth** command.

config wlan security web-auth {{**acl** | **enable** | **disable**} {*wlan_id* | **foreignAp**} [*acl_name* | **none**]} | {**on-macfilter-failure** *wlan_id*} | {**server-precedence** *wlan_id* | **local** | **ldap** | **radius**} | {**flexacl** *wlan_id* [*ipv4_acl_name* | **none**]} | {**ipv6 acl** *wlan_id* [*ipv6_acl_name* |

none] } | { **mac-auth-server** { *ip_address wlan_id* } } | { **timeout** { *value_in_seconds wlan_id* } } | { **web-portal-server** { *ip_address wlan_id* } }

Syntax Description

acl	Configures the access control list.
enable	Enables web authentication.
disable	Disables web authentication.
wlan_id	Wireless LAN identifier from 1 to 512.
foreignAp	Specifies third-party access points.
acl_name	(Optional) ACL name (up to 32 alphanumeric characters).
none	(Optional) Specifies no ACL name.
on-macfilter-failure	Enables web authentication on MAC filter failure.
server-precendence	Configures the authentication server precedence order for Web-Auth users.
local	Specifies the server type.
ldap	Specifies the server type.
radius	Specifies the server type.
flexacl	Configures Flexconnect Access Control List.
ipv4_acl_name	(Optional) IPv4 ACL name. You can enter up to 32 alphanumeric characters.
ipv6_acl_name	(Optional) IPv6 ACL name. You can enter up to 32 alphanumeric characters.
ipv6	Configures IPv6 related parameters.
mac-auth-server	Configures MAC authentication server for the WLAN.
timeout	Configures Local Web authentication Timeout. **Note** The CWA session timeout is fixed to 600 seconds.
value_in_seconds	Timeout value in seconds; valid range is between 300 and 14400 seconds.
web-portal-server	Configures CMCC web portal server for the WLAN.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the security policy for WLAN ID 1 and an ACL named ACL03:

```
(Cisco Controller) >config wlan security web-auth acl 1 ACL03
```

config wlan security web-passthrough acl

To add an access control list (ACL) to the wireless LAN definition, use the **config wlan security web-passthrough acl** command.

config wlan security web-passthrough acl {*wlan_id* | **foreignAp**} {*acl_name* | **none**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
acl_name	ACL name (up to 32 alphanumeric characters).
none	Specifies that there is no ACL.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add an ACL to the wireless LAN definition:

```
(Cisco Controller) >config wlan security web-passthrough acl 1 ACL03
```

config wlan security web-passthrough disable

To disable a web captive portal with no authentication required on a wireless LAN, use the **config wlan security web-passthrough disable** command.

config wlan security web-passthrough disable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to disable a web captive portal with no authentication required on wireless LAN ID 1:

```
(Cisco Controller) >config wlan security web-passthrough disable 1
```

config wlan security web-passthrough email-input

To configure a web captive portal using an e-mail address, use the **config wlan security web-passthrough email-input** command.

config wlan security web-passthrough email-input {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

email-input	Configures a web captive portal using an e-mail address.
enable	Enables a web captive portal using an e-mail address.
disable	Disables a web captive portal using an e-mail address.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure a web captive portal using an e-mail address:

```
(Cisco Controller) >config wlan security web-passthrough email-input enable 1
```

config wlan security web-passthrough enable

To enable a web captive portal with no authentication required on the wireless LAN, use the **config wlan security web-passthrough enable** command.

config wlan security web-passthrough enable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable a web captive portal with no authentication required on wireless LAN ID 1:

```
(Cisco Controller) >config wlan security web-passthrough enable 1
```

config wlan security wpa akm 802.1x

To configure authentication key-management (AKM) using 802.1X, use the **config wlan security wpa akm 802.1x** command.

config wlan security wpa akm 802.1x {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the 802.1X support.
disable	Disables the 802.1X support.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure authentication using 802.1X.

```
(Cisco Controller) >config wlan security wpa akm 802.1x enable 1
```

config wlan security wpa akm cckm

To configure authentication key-management using Cisco Centralized Key Management (CCKM), use the **config wlan security wpa akm cckm** command.

config wlan security wpa akm cckm {**enable** *wlan_id* | **disable** *wlan_id* | *timestamp-tolerance* }

Syntax Description

enable	Enables CCKM support.
disable	Disables CCKM support.
wlan_id	Wireless LAN identifier between 1 and 512.
timestamp-tolerance	CCKM IE time-stamp tolerance. The range is between 1000 to 5000 milliseconds; the default is 1000 milliseconds.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure authentication key-management using CCKM.

```
(Cisco Controller) >config wlan security wpa akm cckm 1500
```

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 wpa akm

To configure Simultaneous Authentication of Equals (SAE) or Opportunistic Wireless Encryption (OWE) Auth Key Management (AKM) for a WLAN, use the **config wlan security wpa akm** command.

config wlan security wpa akm {**sae** | **owe**} {**enable** | **disable**} *wlan-id*

Syntax Description

enable	Enables OWE or SAE AKM support for a WLAN.
disable	Disables OWE or SAE AKM support for a WLAN.
wlan-id	WLAN ID between 1 and 512.

Command Default

None

Command History

Release	Modification
8.10	This command was introduced.

The following example shows how to enable SAE AKM support for a WLAN with ID 2:

```
(Cisco Controller) > config wlan security wpa akm sae enable 2
```

config wlan security wpa akm psk

To configure the Wi-Fi protected access (WPA) preshared key mode, use the **config wlan security wpa akm psk** command.

config wlan security wpa akm psk { { **enable** | **disable** } | { **set-key** *key-format key* } | { **auto-key** { **enable** | **disable** } } | { **pmkid** { **enable** | **disable** } } *wlan_id* }

Syntax Description

enable	Enables WPA-PSK.
disable	Disables WPA-PSK.
set-key	Configures a preshared key.
key-format	Specifies key format. Either ASCII or hexadecimal.
key	WPA preshared key.
auto-key {**enable** | **disable**}	Configures auto PSK on the WLAN.
pmkid {**enable** | **disable**}	Configures PMK ID inclusion in M1 of 4-way handshake messages.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Examples

The following example shows how to configure the WPA preshared key mode:

```
(Cisco Controller) >config wlan security wpa akm psk disable 1
```

config wlan security wpa disable

To disable WPA1, use the **config wlan security wpa disable** command.

config wlan security wpa disable *wlan_id*

Syntax Description

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 disable WPA:

```
(Cisco Controller) >config wlan security wpa disable 1
```

config wlan security wpa enable

To enable WPA1, use the **config wlan security wpa enable** command.

config wlan security wpa enable *wlan_id*

Syntax Description

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 the WPA on WLAN ID 1:

```
(Cisco Controller) >config wlan security wpa enable 1
```

config wlan security wpa ciphers

To configure the Wi-Fi protected authentication (WPA1) or Wi-Fi protected authentication (WPA2), use the **config wlan security wpa ciphers** command.

config wlan security wpa {**wpa1** | **wpa2**} **ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

Syntax Description

wpa1	Configures WPA1 support.
wpa2	Configures WPA2 support.
ciphers	Configures WPA ciphers.
aes	Configures AES encryption support.
tkip	Configures TKIP encryption support.
enable	Enables WPA AES/TKIP mode.
disable	Disables WPA AES/TKIP mode.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

If you are not specifying the WPA versions, it implies the following:

- If the cipher enabled is AES, you are configuring WPA2/AES.
- If the ciphers enabled is AES+TKIP, you are configuring WPA/TKIP, WPA2/AES,or WPA/TKIP.
- If the cipher enabled is TKIP, you are configuring WPA/TKIP or WPA2/TKIP.

You cannot configure TKIP as a standalone encryption method. TKIP can be used only with the AES encryption method.

The following example shows how to encrypt the WPA:

```
(Cisco Controller) >config wlan security wpa wpa1 ciphers aes enable 1
```

config wlan security wpa gtk-random

To enable the randomization of group temporal keys (GTK) between access points and clients on a WLAN, use the **config wlan security wpa gtk-random** command.

config wlan security wpa gtk-random {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the randomization of GTK keys between the access point and clients.
disable	Disables the randomization of GTK keys between the access point and clients.
wlan_id	WLAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When you enable this command, the clients in the Basic Service Set (BSS) get a unique GTK key. The clients do not receive multicast or broadcast traffic.

The following example shows how to enable the GTK randomization for each client associated on a WLAN:

```
(Cisco Controller) >config wlan security wpa gtk-random enable 3
```

config wlan security wpa osen disable

To disable OSU Server-Only Authenticated L2 Encryption Network (OSEN) on a WLAN, use the **config wlan security wpa osen enable** command in WLAN configuration mode.

config wlan security wpa osen disable *wlan-id*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.

Command Default

OSEN is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to disable OSEN on a WLAN:

```
Cisco Controller > config wlan security wpa osen disable 12
```

config wlan security wpa osen enable

To enable OSU Server-Only Authenticated L2 Encryption Network (OSEN) on a WLAN, use the **config wlan security wpa osen enable** command in WLAN configuration mode.

config wlan security wpa osen enable *wlan-id*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.

Command Default OSEN is not enabled.

Command Modes WLAN configuration

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to enable an OSEN on a WLAN:

```
Cisco Controller > config wlan security wpa osen enable 12
```

config wlan security wpa wpa1 disable

To disable WPA1, use the **config wlan security wpa wpa1 disable** command.

config wlan security wpa wpa1 disable *wlan_id*

Syntax Description

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 disable WPA1:

```
(Cisco Controller) >config wlan security wpa wpa1 disable 1
```

config wlan security wpa wpa1 enable

To enable WPA1, use the **config wlan security wpa wpa1 enable** command.

config wlan security wpa wpa1 enable *wlan_id*

Syntax Description

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 enable WPA1:

```
(Cisco Controller) >config wlan security wpa wpa1 enable 1
```

config wlan security wpa wpa2 disable

To disable WPA2, use the **config wlan security wpa wpa2 disable** command.

config wlan security wpa wpa2 disable *wlan_id*

Syntax Description

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 disable WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 disable 1
```

config wlan security wpa wpa2 enable

To enable WPA2, use the **config wlan security wpa wpa2 enable** command.

config wlan security wpa wpa2 enable *wlan_id*

Syntax Description

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 enable WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 enable 1
```

config wlan security wpa wpa2 cache

To configure caching methods on a WLAN, use the **config wlan security wpa wpa2 cache** command.

config wlan security wpa wpa2 cache sticky {**enable** | **disable**} *wlan_id*

Syntax Description

sticky	Configures Sticky Key Caching (SKC) roaming support on the WLAN.
enable	Enables SKC roaming support on the WLAN.
disable	Disables SKC roaming support on the WLAN.

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

In SKC (Sticky Key caching) also known as PKC (Pro Active Key caching), the client stores each Pairwise Master Key (PMK) ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has a PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs.

The following example shows how to enable SKC roaming support on a WLAN:

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 1
```

config wlan security wpa wpa2 cache sticky

To configure Sticky PMKID Caching (SKC) on a WLAN, use the **config wlan security wpa wpa2 cache sticky** command.

config wlan security wpa wpa2 cache sticky {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables SKC on a WLAN.
disable	Disables SKC on a WLAN.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

Stkcky PMKID Caching is disabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The controller supports Sticky PMKID Caching (SKC). With sticky PMKID caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client. In SKC also known as PKC (Pro Active Key caching), the client stores each Pairwise Master Key (PMK) ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

- You cannot use SKC for large scale deployments as the controller supports SKC only up to eight APs.
- SKC does not work across controllers in a mobility group.
- SKC works only on WPA2-enabled WLANs.

- SKC works only on local mode APs.

The following example shows how to enable Sticky PMKID Caching on WLAN 5:

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 5
```

config wlan security wpa wpa2 ciphers

To configure WPA2 ciphers and enable or disable Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) data encryption for WPA2, use the **config wlan security wpa wpa2 ciphers** command

config wlan security wpa wpa2 ciphers {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

Syntax Description

(Cisco Controller) > **aes**	Configures AES data encryption for WPA2.
tkip	Configures TKIP data encryption for WPA2.
enable	Enables AES or TKIP data encryption for WPA2.
disable	Disables AES or TKIP data encryption for WPA2.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

AES is enabled by default.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable AES data encryption for WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1
```

config wlan security wpa3

To configure WPA3 on a WLAN, use the **config wlan security wpa wpa3** command.

config wlan security wpa wpa3 {**enable** | **disable**} *wlan-id*

Syntax Description

enable	Enables WPA3 on a WLAN.
disable	Disables WPA3 on a WLAN.
wlan-id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
8.10	This command was introduced.

Examples

The following example shows you how to enable WPA3 on a WLAN whose ID is 4:

```
(Cisco Controller) > config wlan security wpa wpa3 enable 4
```

config wlan ssid

To edit an SSID associated to a WLAN, use the **config wlan ssid** command.

config wlan ssid *wlan_id ssid*

Syntax Description

wlan_id	WLAN identifier from 1 to 512.
ssid	Service Set Identifier (SSID) associated to a WLAN.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to edit an SSID associated to a WLAN:

```
(Cisco Controller) >config wlan disable 1
(Cisco Controller) >config wlan ssid 1 new_samp
(Cisco Controller) >show wlan summary
Number of WLANs.................................. 1

WLAN ID  WLAN Profile Name / SSID   Status    Interface Name   PMIPv6 Mobility
-------  -------------------------  -------  -----------------  ---------------
1        sample / new_samp          Disabled   management            none
```

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 uapsd compliant client enable

To enable WPA1, use the **config wlan uapsd compliant-client enable** command.

Note This was introduced for Ascom non-wmm capable phones and is not applicable for Cisco 792x/9971 IP phones.

config wlan uapsd compliant-client enable*wlan-id*

Syntax Description

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 enable WPA1:

```
(Cisco Controller) >config wlan uapsd compliant-client enable 1
```

Property Type	Property Value	Property Description

config wlan uapsd compliant-client disable

To disable WPA1, use the **config wlan uapsd compliant-client disable** command.

Note This was introduced for Ascom non-wmm capable phones and is not applicable for Cisco 792x/9971 IP phones.

config wlan uapsd compliant-client disable*wlan-id*

Syntax Description

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 enable WPA1:

```
(Cisco Controller) >config wlan uapsd compliant-client disable 1
```

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 webauth-exclude

To release the guest user IP address when the web authentication policy time expires and exclude the guest user from acquiring an IP address for three minutes, use the **config wlan webauth-exclude** command.

config wlan webauth-exclude *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier (1 to 512).
enable	Enables web authentication exclusion.
disable	Disables web authentication exclusion.

Command Default Disabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines You can use this command for guest WLANs that are configured with web authentication.

This command is applicable when you configure the internal DHCP scope on the controller.

By default, when the web authentication timer expires for a guest user, the guest user can immediately reassociate with the same IP address before another guest user can acquire the IP address. If there are many guest users or limited IP address in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user's IP address is released when the web authentication policy time expires and the guest user is excluded from acquiring an IP address for three minutes. The IP address is available for another guest user to use. After three minutes, the excluded guest user can reassociate and acquire an IP address, if available.

The following example shows how to enable the web authentication exclusion for WLAN ID 5:

```
(Cisco Controller) >config wlan webauth-exclude 5 enable
```

config wlan wifidirect

To configure Wi-Fi Direct Client Policy on a WLAN, use the **config wlan wifidirect** command.

config wlan wifidirect {**allow** | **disable** | **not-allow** | **xconnect-not-allow**} *wlan_id*

Syntax Description

allow	Allows Wi-Fi Direct clients to associate with the WLAN
disable	Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate
not-allow	
xconnect-not-allow	Disallows the Wi-Fi Direct clients from associating with the WLAN
wlan_id	Wireless LAN identifier (1 to 16).

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to allow Wi-Fi Direct Client Policy on WLAN ID 1:

```
(Cisco Controller) >config wlan wifidirect allow 1
```

config wlan wmm

To configure Wi-Fi Multimedia (WMM) mode on a wireless LAN, use the **config wlan wmm** command.

config wlan wmm {**allow** | **disable** | **require**} *wlan_id*

Syntax Description

allow	Allows WMM on the wireless LAN.
disable	Disables WMM on the wireless LAN.
require	Specifies that clients use WMM on the specified wireless LAN.
wlan_id	Wireless LAN identifier (1 to 512).

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When the controller is in Layer 2 mode and WMM is enabled, you must put the access points on a trunk port in order to allow them to join the controller.

The following example shows how to configure wireless LAN ID 1 to allow WMM:

```
(Cisco Controller) >config wlan wmm allow 1
```

The following example shows how to configure wireless LAN ID 1 to specify that clients use WMM:

```
(Cisco Controller) >config wlan wmm require 1
```

transfer download datatype icon

To download icon from TFTP or FTP server onto the controller, use the **transfer download datatype icon** command.

transfer download datatype icon

Syntax Description

None

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Example

This example shows how to download icon from TFTP or FTP server onto the controller:

```
Cisco Controller > transfer download datatype icon
```

debug Commands

This section lists the **debug** commands to manage debugging of WLANs managed by the controller.

Caution Debug commands are reserved for use only under the direction of Cisco personnel. Do not use these commands without direction from Cisco-certified staff.

debug 11v all

To configure the 802.11v debug options, use the **debug 11v all** command.

debug 11v all {**enable | disable**}

Syntax Description

enable	Enables all the debug.
disable	Disables all the debug.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable all the debug:

```
(Cisco Controller) >debug 11v all enable
```

debug 11v detail

To configure the 802.11v debug details, use the **debug 11v detail** command.

debug 11v detail {**enable | disable**}

Syntax Description

enable	Enables debug details.
disable	Disables debug details.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable 802.11v debug details:

```
(Cisco Controller) >debug 11v detail enable
```

debug 11v error

To configure the 802.11v error debug options, use the **debug 11v errors** command.

debug 11v errors {**enable | disable**}

Syntax Description

enable	Enables error debug.
disable	Disables error debug.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable 802.11v error debug:

```
(Cisco Controller) >debug 11v error enable
```

debug client

To configure the debugging of a passive client that is associated correctly with the access point, use the **debug client** command.

debug client *mac_address*

Syntax Description

mac_address	MAC address of the client.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to debug a passive client with MAC address 00:0d:28:f4:c0:45:

```
(Cisco Controller) >debug client 00:0d:28:f4:c0:45
```

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 ft

To configure debugging of 802.11r, use the **debug ft** command.

debug ft {**events** | **keys**} {**enable** | **disable**}

Syntax Description

events	Configures debugging of the 802.11r events.
keys	Configures debugging of the 802.11r keys.
enable	Enables debugging of the 802.11r options.
disable	Disables debugging of the 802.11r options.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable 802.11r debugging:

```
(Cisco Controller) >debug ft events enable
```

debug profiling

To configure the debugging of client profiling, use the **debug profiling** command.

debug profiling {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of client profiling (HTTP and DHCP profiling).
disable	Disables the debugging of client profiling (HTTP and DHCP profiling).

Command Default

Disabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging of client profiling:

```
(Cisco Controller) >debug profiling enable
```

test Commands

This section lists the **test** commands for WLANs.

test pmk-cache delete

To delete an entry in the Pairwise Master Key (PMK) cache from all Cisco wireless LAN controllers in the mobility group, use the **test pmk-cache delete** command.

test pmk-cache delete [**all** | *mac_address*] { **local** | **global** }

Syntax Description

all	Deletes PMK cache entries from all controllers.
mac_address	MAC address of the controller from which PMK cache entries have to be deleted.
local	Deletes PMK cache entries only on this controller (default)
global	Deletes PMK cache entries, for clients currently connected to this controller, across the mobility group

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to delete all entries in the PMK cache:

```
(Cisco Controller) >test pmk-cache delete all
```

LWAP Commands

capwap ap controller ip address

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

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

Syntax Description

A.B.C.D	IP address of the controller.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

capwap ap dot1x

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

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

Syntax Description

user_name	Dot1x username.
password	Dot1x password.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

capwap ap hostname

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

capwap ap hostname *host_name*

Syntax Description

host_name	Hostname of the access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

```
ap_console >capwap ap hostname controller
```

capwap ap ip address

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

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

Syntax Description

A.B.C.D	IP address.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

capwap ap ip default-gateway

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

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

Syntax Description

A.B.C.D	Default gateway address of the capwap access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

capwap ap log-server

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

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

Syntax Description

A.B.C.D	IP address of the syslog server.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

capwap ap primary-base

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

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

However, this command configures only the IPv4 address for a Cisco Wave 1 AP. To configure Cisco Wave 1 APs with IPv6 address refer the command **capwap ap ipv6 primary-base**

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

Syntax Description

WORD	Name of the primary controller.
A.B.C.D	IP address of the primary controller.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

capwap ap primed-timer

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

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

Syntax Description

enable	Enables the primed timer settings
disable	Disables the primed timer settings.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

lwapp ap controller ip address

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

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

Syntax Description

A.B.C.D	IP address of the controller.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

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

config 802.11-a antenna extAntGain

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

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

Syntax Description

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

Command Default

Channel properties are disabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

Related Topics

config 802.11-a channel ap, on page 531

config 802.11-a channel ap

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

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

Syntax Description

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

Command Default

Channel properties are disabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to set the channel properties:

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

Related Topics

config 802.11-a antenna extAntGain, on page 530
config 802.11-a, on page 685

config 802.11-a txpower ap

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

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

Syntax Description

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

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

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

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

Related Topics

config 802.11-a antenna extAntGain, on page 530
config 802.11-a, on page 685
config 802.11-a channel ap, on page 531

config 802.11 antenna diversity

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the diversity.
sideA	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point left port.
sideB	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point right port.
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 enable antenna diversity for AP01 on an 802.11b network:

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

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

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

Related Topics

config 802.11-a, on page 685

config 802.11 antenna extAntGain

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

Related Topics

config 802.11-a, on page 685

config 802.11 antenna mode

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
omni	Specifies to use both internal antennas.
sectorA	Specifies to use only the side A internal antenna.
sectorB	Specifies to use only the side B internal antenna.
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 access point AP01 antennas for a 360-degree omnidirectional pattern on an 802.11b network:

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

Related Topics

config 802.11-a, on page 685

config 802.11 antenna selection

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
internal	Specifies the internal antenna.
external	Specifies the external antenna.
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 access point AP02 on an 802.11b network to use the internal antenna:

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

Related Topics

config 802.11-a, on page 685

config 802.11 beamforming

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

Follow these guidelines for using Beamforming:

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

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

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

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

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

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

config 802.11 disable

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

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

Syntax Description

a	Configures the 802.11a on slot 1 and 802.11ac/ax 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 advanced 802.11 profile clients

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access points.
cisco_ap	Cisco lightweight access point name.
clients	802.11a Cisco lightweight access point client threshold between 1 and 75 clients.

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

config advanced 802.11 profile customize

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

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

Syntax Description

a	Specifies the 802.11a/n network.
b	Specifies the 802.11b/g/n network.
cisco_ap	Cisco lightweight access point.
on	Customizes performance profiles for this Cisco lightweight access point.
off	Uses global default performance profiles for this Cisco lightweight access point.

Command Default

The default state of performance profile customization is Off.

Command History

Release	Modification
8.3	This command was introduced.

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

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

config advanced 802.11 profile foreign

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access points.
cisco_ap	Cisco lightweight access point name.
percent	802.11a foreign 802.11a interference threshold between 0 and 100 percent.

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

Related Topics

config advanced 802.11 profile throughput, on page 543

config advanced 802.11 profile noise

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

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

Syntax Description

a	Specifies the 802.11a/n network.
b	Specifies the 802.11b/g/n network.
global	Configures all 802.11a Cisco lightweight access point specific profiles.
cisco_ap	Cisco lightweight access point name.
dBm	802.11a foreign noise threshold between –127 and 0 dBm.

Command Default

The default foreign noise threshold value is –70 dBm.

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

Related Topics

config advanced 802.11 profile throughput, on page 543
config advanced 802.11 profile foreign, on page 541

config advanced 802.11 profile throughput

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

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

Syntax Description

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

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

Related Topics

config advanced 802.11 profile foreign, on page 541

config advanced 802.11 profile utilization

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures a global Cisco lightweight access point specific profile.
cisco_ap	Cisco lightweight access point name.
percent	802.11a RF utilization threshold between 0 and 100 percent.

Command Default

The default RF utilization threshold value is 80 percent.

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

Related Topics

config advanced 802.11 profile throughput, on page 543
config advanced 802.11 profile foreign, on page 541

config advanced backup-controller secondary

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

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

Syntax Description

system name	Configures primary|secondary backup controller.
IP addr	IP address of the backup controller.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

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

Related Commands

show advanced back-up controller

config advanced client-handoff

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

config advanced client-handoff *num_of_retries*

Syntax Description

num_of_retries	Number of excessive retries before client handoff (from 0 to 255).

Command Default

The default value for the number of 802.11 data packet excessive retries is 0.

Command History

Release	Modification
8.3	This command was introduced.

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

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

config advanced dot11-padding

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

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

Syntax Description

enable	Enables the over-the-air frame padding.
disable	Disables the over-the-air frame padding.

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

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

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

Related Commands

debug dot11

debug dot11 mgmt interface

debug dot11 mgmt msg

debug dot11 mgmt ssid

debug dot11 mgmt state-machine

debug dot11 mgmt station

show advanced dot11-padding

Related Topics

config client location-calibration, on page 743

config advanced assoc-limit

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

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

Syntax Description

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

Command Default

The default state of the command is disabled state.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

config advanced max-1x-sessions

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

config advanced max-1x-sessions *no_of_sessions*

Syntax Description

no_of_sessions	Number of maximum 802.1x session initiation per AP at a time. The range is from 0 to 255, where 0 indicates unlimited.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

config advanced probe backoff

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

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

Syntax Description

enable	To use default backoff parameter value for probe response.
disable	To use increased backoff parameters for probe response.

Command Default

Disabled

Command History

Release	Modification
8.3	This command was introduced.

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

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

config advanced probe filter

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

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

Syntax Description

enable	Enables the filtering of probe requests.
disable	Disables the filtering of probe requests.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

config advanced probe limit

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

config advanced probe limit *num_probes interval*

Syntax Description

num_probes	Number of probe requests (from 1 to 100) forwarded to the controller per client per access point radio in a given interval.
interval	Probe limit interval (from 100 to 10000 milliseconds).

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

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

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

config advanced timers

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

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

Syntax Description

ap-coverage-report	Configures RRM coverage report interval for all APs.
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 controller 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 Controller.

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

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

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

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

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

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

config ap

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

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

Syntax Description

enable	Enables the Cisco lightweight access point.
disable	Disables the Cisco lightweight access point.
cisco_ap	Name of the Cisco lightweight access point.
add	Adds foreign access points.
delete	Deletes foreign access points.
MAC	MAC address of a foreign access point.
port	Port number through which the foreign access point can be reached.
IP_address	IP address of the foreign access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

config ap cdp

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

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

Syntax Description

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

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

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

config ap core-dump

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

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

Syntax Description

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

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

config ap crash-file clear-all

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

config ap crash-file clear-all

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to delete all crash files:

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

config ap crash-file delete

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

config ap crash-file delete *filename*

Syntax Description

filename	Name of the file to delete.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to delete crash file 1:

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

config ap crash-file get-crash-file

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

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

Syntax Description

cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Use the **transfer upload datatype** command to transfer the collected data to the Cisco wireless LAN controller.

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

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

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

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

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

Syntax Description

slot_id	Slot ID (either 0 or 1).
cisco_ap	Name of a Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

config ap ethernet tag

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

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

Syntax Description

id	Specifies the VLAN id.
vlan_id	ID of the trunk VLAN.
disable	Disables the VLAN tag feature. When you disable VLAN tagging, the access point untags the CAPWAP packets.
cisco_ap	Name of the Cisco AP.
all	Configures VLAN tagging on all the Cisco access points.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

After you configure VLAN tagging, the configuration comes into effect only after the access point reboots.

You cannot configure VLAN tagging on mesh access points.

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

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

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

config ap image swap

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

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

Syntax Description

cisco_ap	Name of a Cisco lightweight access point.
all	Specifies all access points to interchange the boot images.

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

config ap led-state

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

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

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

Syntax Description

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

Usage Guidelines

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

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

config ap location

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

config ap location *location cisco_ap*

Syntax Description

location	Location name of the access point (enclosed by double quotation marks).
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

config ap logging syslog level

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

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

Syntax Description

severity_level	Severity levels are as follows: • emergencies—Severity level 0 • alerts—Severity level 1 • critical—Severity level 2 • errors—Severity level 3 • warnings—Severity level 4 • notifications—Severity level 5 • informational—Severity level 6 • debugging—Severity level 7
cisco_ap	Cisco access point.
all	Specifies all access points.

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

config ap mgmtuser add

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

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

Syntax Description

username	Configures the username for AP management.
AP_username	Management username.
password	Configures the password for AP management.
AP_password	AP management password.
secret	Configures the secret password for privileged AP management.
secret	AP managemetn secret password.
all	Applies configuration to every AP that does not have a specific username.
cisco_ap	Cisco access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The following requirements are enforced on the password:

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

The following requirement is enforced on the secret password:

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

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

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

config ap mgmtuser delete

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

config ap mgmtuser delete *cisco_ap*

Syntax Description

cisco_ap	Access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

config ap monitor-mode

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

config ap name

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

config ap name *new_name old_name*

Syntax Description

new_name	Desired Cisco lightweight access point name.
old_name	Current Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

config ap packet-dump

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

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

Syntax Description

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

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

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Packet Capture does not work during intercontroller roaming.

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

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

This command supports both IPv4 and IPv6 address formats.

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

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

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

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

config ap port

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

config ap port *MAC port*

Syntax Description

MAC	Foreign access point MAC address.
port	Port number for accessing the foreign access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

config ap power injector

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

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

Syntax Description

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

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

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

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

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

config ap power pre-standard

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

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

Syntax Description

enable	Enables the inline power Cisco pre-standard switch state for an access point.
disable	Disables the inline power Cisco pre-standard switch state for an access point.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

Disabled.

Command History

Release	Modification
8.3	This command was introduced.

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

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

config ap preferred-mode

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Example

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

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

config ap primary-base

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

This command supports both IPv4 and IPv6 address formats.

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

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

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

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

Related Commands

show ap config general

config ap reporting-period

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

config ap reporting-period *period*

Syntax Description

period	Time period in seconds between 10 and 120.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

config ap reset

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

config ap reset *cisco_ap*

Syntax Description

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 reset an access point:

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

config ap retransmit interval

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

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

Syntax Description

seconds	AP control packet retransmission timeout between 2 and 5 seconds.
all	Specifies all access points.
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 the retransmission interval for all access points globally:

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

config ap retransmit count

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

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

Syntax Description

count	Number of times control packet will be retransmitted. The range is from 3 to 8.
all	Specifies all access points.
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 the retransmission retry count for a specific access point:

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

config ap sniff

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

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

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
enable	Enables sniffing on an access point.
channel	Channel to be sniffed.
server_ip	IP address of the remote machine running Omnipeek, Airopeek,AirMagnet, or Wireshark software.
disable	Disables sniffing on an access point.
cisco_ap	Access point configured as the sniffer.

Command Default

Channel 36.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

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

config ap ssh

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

config ap static-ip

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

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

Syntax Description

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

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

This command supports both IPv4 and IPv6 address formats.

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

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

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

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

Related Commands

show ap config general

config ap stats-timer

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

config ap stats-timer *period cisco_ap*

Syntax Description

period	Time in seconds from 0 to 65535. A zero value disables the timer.
cisco_ap	Cisco lightweight access point name.

Command Default

The default value is 0 (disabled state).

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

config ap syslog host global

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

config ap syslog host global *ip_address*

Syntax Description

ip_address	IPv4/IPv6 address of the syslog server.

Command Default

The default value of the IPv4 address of the syslog server is 255.255.255.255.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

This command supports both IPv4 and IPv6 address formats.

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

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

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

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

config ap syslog host specific

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

config ap syslog host specific *ap_nameip_address*

Syntax Description

ap_name	Cisco lightweight access point.
ip_address	IPv4/IPv6 address of the syslog server.

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure a syslog server:

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

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

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

config ap tcp-mss-adjust

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

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

Syntax Description

enable	Enables the TCP maximum segment size on an access point.
disable	Disables the TCP maximum segment size on an access point.
cisco_ap	Cisco access point name.
all	Specifies all access points.
size	Maximum segment size. • IPv4—Specify a value between 536 and 1363. • IPv6—Specify a value between 1220 and 1331. **Note** Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP.

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

config ap telnet

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

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

config ap timezone

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

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

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

Example

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

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

config ap username

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

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

Syntax Description

user_id	Administrator username.
passwd	Administrator password.
all	(Optional) Specifies all access points.
ap_name	Name of a specific access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

```
(Cisco Controller) > config ap username jack password blue la204
```

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

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

config ap venue

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

Table 3: Venue Group Mapping

Venue Group Name	Value	Venue Type for Group
UNSPECIFIED	0	

Venue Group Name	Value	Venue Type for Group
ASSEMBLY	1	• 0—UNSPECIFIED ASSEMBLY • 1—ARENA • 2—STADIUM • 3—PASSENGER TERMINAL (E.G., AIRPORT, BUS, FERRY, TRAIN STATION) • 4—AMPHITHEATER • 5—AMUSEMENT PARK • 6—PLACE OF WORSHIP • 7—CONVENTION CENTER • 8—LIBRARY • 9—MUSEUM • 10—RESTAURANT • 11—THEATER • 12—BAR • 13—COFFEE SHOP • 14—ZOO OR AQUARIUM • 15—EMERGENCY COORDINATION CENTER
BUSINESS	2	• 0—UNSPECIFIED BUSINESS • 1—DOCTOR OR DENTIST OFFICE • 2—BANK • 3—FIRE STATION • 4—POLICE STATION • 6—POST OFFICE • 7—PROFESSIONAL OFFICE • 8—RESEARCH AND DEVELOPMENT FACILITY • 9—ATTORNEY OFFICE

Venue Group Name	Value	Venue Type for Group
EDUCATIONAL	3	• 0—UNSPECIFIED EDUCATIONAL • 1—SCHOOL, PRIMARY • 2—SCHOOL, SECONDARY • 3—UNIVERSITY OR COLLEGE
FACTORY-INDUSTRIAL	4	• 0—UNSPECIFIED FACTORY AND INDUSTRIAL • 1—FACTORY
INSTITUTIONAL	5	• 0—UNSPECIFIED INSTITUTIONAL • 1—HOSPITAL • 2—LONG-TERM CARE FACILITY (E.G., NURSING HOME, HOSPICE, ETC.) • 3—ALCOHOL AND DRUG RE-HABILITATION CENTER • 4—GROUP HOME • 5—PRISON OR JAIL
MERCANTILE	6	• 0—UNSPECIFIED MERCANTILE • 1—RETAIL STORE • 2—GROCERY MARKET • 3—AUTOMOTIVE SERVICE STATION • 4—SHOPPING MALL • 5—GAS STATION
RESIDENTIAL	7	• 0—UNSPECIFIED RESIDENTIAL • 1—PRIVATE RESIDENCE • 2—HOTEL OR MOTEL • 3—DORMITORY • 4—BOARDING HOUSE
STORAGE	8	UNSPECIFIED STORAGE

Venue Group Name	Value	Venue Type for Group
UTILITY-MISC	9	0—UNSPECIFIED UTILITY AND MISCELLANEOUS
VEHICULAR	10	• 0—UNSPECIFIED VEHICULAR • 1—AUTOMOBILE OR TRUCK • 2—AIRPLANE • 3—BUS • 4—FERRY • 5—SHIP OR BOAT • 6—TRAIN • 7—MOTOR BIKE
OUTDOOR	11	• 0—UNSPECIFIED OUTDOOR • 1—MUNI-MESH NETWORK • 2—CITY PARK • 3—REST AREA • 4—TRAFFIC CONTROL • 5—BUS STOP • 6—KIOSK

config ap wlan

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

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

Syntax Description

enable	Enables the wireless LAN override on an access point.
disable	Disables the wireless LAN override on an access point.
802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
wlan_id	Cisco wireless LAN controller ID assigned to a wireless LAN.
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 enable wireless LAN override on the AP03 802.11a radio:

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

config country

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

config country *country_code*

Syntax Description

country_code	Two-letter or three-letter country code.

Command Default

us (country code of the United States of America).

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

config known ap

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

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

Syntax Description

add	Adds a new known access point entry.
alert	Generates a trap upon detection of the access point.
delete	Deletes an existing known access point entry.
MAC	MAC address of the known Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

clear ap config

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

clear ap config *ap_name*

Syntax Description

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 ap tsm

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

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

Syntax Description

802.11a	Clears 802.11a TSM statistics of clients associated to an access point.
802.11b	Clears 802.11b TSM statistics of clients associated to an access point.
cisco_ap	Cisco lightweight access point.
all	Clears TSM statistics of clients associated to the access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

debug ap

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

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

Syntax Description

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

Command Default

The remote debugging of Cisco lightweight access points is disabled.

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

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

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

debug ap enable

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

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

Syntax Description

enable	Enables the remote debugging. **Note** The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
disable	Disables the remote debugging.
command	Specifies that a CLI command is to be executed on the access point.
cmd	Command to be executed. **Note** The command to be executed must be enclosed in double quotes, such as **debug ap command "led flash 30" AP03**. The output of the command displays only to the controller console and does not send output to a controller Telnet/SSH CLI session.
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 enable the remote debugging on access point AP01:

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

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

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

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

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

debug ap packet-dump

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

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

Syntax Description

enable	Enables the debugging of Packet Capture of an access point.
disable	Disables the debugging of Packet Capture of an access point.

Command Default

Debugging of Packet Capture is disabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Packet Capture does not work during inter-controller roaming.

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

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

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

debug ap show stats

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

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

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

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

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

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

debug ap show stats video

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

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

Syntax Description

cisco_ap	Cisco lightweight access point name.
multicast mgid	Displays multicast database related information for the specified MGID of an access point.
mgid_value	Layer 2 MGID database number from 1 to 4095.
admission	Displays the video admission control.
bandwidth	Displays the video bandwidth.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

debug capwap

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

debug lwapp console cli

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

debug lwapp console cli

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

debug service ap-monitor

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

reset system at

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

Related Topics

reset system in, on page 211
reset system notify-time, on page 212

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 211
reset system notify-time, on page 212

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 211
reset system in, on page 211
reset system notify-time, on page 212

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
```

show advanced max-1x-sessions

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

show advanced max-1x-sessions

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show advanced probe

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

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show advanced timers

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

show advanced timers

Syntax Description

This command has no arguments or keywords.

Command Default

The defaults are shown in the “Examples” section.

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap auto-rf

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
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 display auto-RF information for an access point:

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

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

show ap cdp

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

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

Syntax Description

all	Displays the CDP status on all access points.
ap-name	Displays the CDP status for a specified access point.
cisco_ap	Specified access point name.
neighbors	Displays neighbors using CDP.
detail	Displays details about a specific access point neighbor using CDP.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

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

```
(Cisco Controller) >show ap cdp neighbor all
AP Name     AP IP            Neighbor Name       Neighbor IP      Neighbor Port
---------   --------------   ------------------  --------------   -------------
SB_RAP1     192.168.102.154  sjc14-41a-sw1       192.168.102.2    GigabitEthernet1/0/13
```

```
SB_RAP1     192.168.102.154  SB_MAP1             192.168.102.137  Virtual-Dot11Radio0
SB_MAP1     192.168.102.137  SB_RAP1             192.168.102.154  Virtual-Dot11Radio0
SB_MAP1     192.168.102.137  SB_MAP2             192.168.102.138  Virtual-Dot11Radio0
SB_MAP2     192.168.102.138  SB_MAP1             192.168.102.137  Virtual-Dot11Radio1
SB_MAP2     192.168.102.138  SB_MAP3             192.168.102.139  Virtual-Dot11Radio0
SB_MAP3     192.168.102.139  SB_MAP2             192.168.102.138  Virtual-Dot11Radio1
```

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

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

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

```
(Cisco Controller) >show ap cdp neighbors detail SB_MAP2
AP Name:SB_MAP2
AP IP address:192.168.102.138
-------------------------
Device ID: SB_MAP1
Entry address(es): 192.168.102.137
Platform: cisco AIR-LAP1522AG-A-K9  ,  Cap
Interface: Virtual-Dot11Radio0,  Port ID (outgoing port): Virtual-Dot11Radio1
Holdtime : 180 sec
Version :
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Experimental Version 12.4(200
81114:084420) [BLD-v124_18a_ja_throttle.20081114 208] Copyright (c) 1986-2008 by
 Cisco Systems, Inc. Compiled Fri 14-Nov-08 23:08 by
advertisement version: 2
-------------------------
Device ID: SB_MAP3
Entry address(es): 192.168.102.139
Platform: cisco AIR-LAP1522AG-A-K9  ,  Capabilities: Trans-Bridge
Interface: Virtual-Dot11Radio1,  Port ID (outgoing port): Virtual-Dot11Radio0
Holdtime : 180 sec
Version :
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Experimental Version 12.4(200
81114:084420) [BLD-v124_18a_ja_throttle.20081114 208] Copyright (c) 1986-2008 by
 Cisco Systems, Inc. Compiled Fri 14-Nov-08 23:08 by
advertisement version: 2
```

show ap channel

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

show ap channel *ap_name*

Syntax Description

ap_name	Name of the mesh access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap config

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

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

Syntax Description

802.11a	Specifies the 802.11a or 802.11b/g network.
802.11b	Specifies the 802.11b/g network.
summary	(Optional) Displays radio summary of all APs
cisco_ap	Lightweight access point name.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

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

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

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

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

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

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

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

show ap config general

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

show ap config general *ap-name*

Syntax Description

ap-name	AP name

Command History

Release	Modification
8.3	This command was introduced.

show ap config global

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

show ap config global

Syntax Description

This command has no arguments and keywords.

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap core-dump

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

show ap core-dump *cisco_ap*

Syntax Description

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 display memory core dump information:

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

show ap crash-file

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

show ap crash-file

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap data-plane

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

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

Syntax Description

all	Specifies all Cisco lightweight access points.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap dtls-cipher-suite

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

show ap dtls-cipher-suite

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap ethernet tag

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

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

Syntax Description

summary	Displays the VLAN tagging information for all access points associated to the controller.
cisco_ap	Name of the Cisco lightweight access point. Displays the VLAN tagging information for a specific access point associated to the controller.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

show ap eventlog

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

show ap eventlog *ap_name*

Syntax Description

ap_name	Event log for the specified access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap image

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

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

Syntax Description

cisco_ap	Name of the lightweight access point.
all	Specifies all access points.

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

Command History

Release	Modification
8.3	This command was introduced.

show ap inventory

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

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

Syntax Description

ap-name	Inventory for the specified AP.
all	Inventory for all the APs.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap join stats detailed

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

show ap join stats detailed *ap_mac*

Syntax Description

ap_mac	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap join stats summary

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

show ap join stats summary *ap_mac*

Syntax Description

ap_mac	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

To obtain the MAC address of the 802.11 radio interface, enter the **show interface** command on the access point.

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

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

show ap join stats summary all

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

show ap join stats summary all

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap led-state

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

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

Syntax Description

all	Shows the LED state for all access points.
cisco_ap	Name of the access point whose LED state is to be shown.

Command Default

The AP LED state is enabled.

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap led-flash

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

show ap led-flash *cisco_ap*

Syntax Description

cisco_ap	Enter the name of the Cisco AP.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap max-count summary

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

show ap max-count summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

```
(Cisco Controller) >show ap max-count

The max number of AP's supported.................. 500
```

Related Topics

config ap max-count

show ap monitor-mode summary

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

show ap monitor-mode summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap module summary

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

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

Syntax Description

ap-name	Cisco AP name that has the external module
all	All Cisco APs that have the external module

Command History

Release	Modification
8.3	This command was introduced.

show ap packet-dump status

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

show ap packet-dump status

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Packet Capture does not work during intercontroller roaming.

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

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

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

show ap prefer-mode stats

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

show ap prefer-mode stats

Syntax Description

stats	Displays prefer-mode global and per AP group statistics

Command History

Release	Modification
8.3	This command was introduced.

show ap retransmit

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

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

Syntax Description

all	Specifies all access points.
cisco_ap	Name of the access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

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

show ap stats

To display the statistics for a Cisco lightweight access point, use the **show ap stats** command.

show ap stats {**802.11**{**a** | **b**} | **wlan** | **ethernet summary**} *cisco_ap* [**tsm** {*client_mac* | **all**}]

Syntax Description

802.11a	Specifies the 802.11a network
802.11b	Specifies the 802.11b/g network.
wlan	Specifies WLAN statistics.
ethernet	Specifies AP ethernet interface statistics.
summary	Displays ethernet interface summary of all the connected Cisco access points.
cisco_ap	Name of the lightweight access point.
tsm	(Optional) Specifies the traffic stream metrics.
client_mac	(Optional) MAC address of the client.
all	(Optional) Specifies all access points.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display statistics of an access point for the 802.11b network:

```
(Cisco Controller) >show ap stats 802.11a Ibiza

Number Of Slots.................................. 2
AP Name.......................................... Ibiza
MAC Address...................................... 44:2b:03:9a:8a:73
Radio Type....................................... RADIO_TYPE_80211a
Stats Information
  Number of Users................................ 0
  TxFragmentCount................................ 84628
  MulticastTxFrameCnt............................ 84628
  FailedCount.................................... 0
  RetryCount..................................... 0
  MultipleRetryCount............................. 0
  FrameDuplicateCount............................ 0
  RtsSuccessCount................................ 1
  RtsFailureCount................................ 0
  AckFailureCount................................ 0
  RxIncompleteFragment........................... 0
  MulticastRxFrameCnt............................ 0
  FcsErrorCount.................................. 20348857
  TxFrameCount................................... 84628
```

```
  WepUndecryptableCount..................... 19907
  TxFramesDropped........................... 0
OEAP WMM Stats :
  Best Effort:
    Tx Frame Count.......................... 0
    Tx Failed Frame Count................... 0
    Tx Expired Count........................ 0
    Tx Overflow Count....................... 0
    Tx Queue Count.......................... 0
    Tx Queue Max Count...................... 0
    Rx Frame Count.......................... 0
    Rx Failed Frame Count................... 0
  Background:
    Tx Frame Count.......................... 0
    Tx Failed Frame Count................... 0
    Tx Expired Count........................ 0
    Tx Overflow Count....................... 0
    Tx Queue Count.......................... 0
    Tx Queue Max Count...................... 0
    Rx Frame Count.......................... 0
    Rx Failed Frame Count................... 0
  Video:
    Tx Frame Count.......................... 0
    Tx Failed Frame Count................... 0
    Tx Expired Count........................ 0
    Tx Overflow Count....................... 0
    Tx Queue Count.......................... 0
    Tx Queue Max Count...................... 0
    Rx Frame Count.......................... 0
    Rx Failed Frame Count................... 0
  Voice:
    Tx Frame Count.......................... 0
    Tx Failed Frame Count................... 0
    Tx Expired Count........................ 0
    Tx Overflow Count....................... 0
    Tx Queue Count.......................... 0
    Tx Queue Max Count...................... 0
    Rx Frame Count.......................... 0
    Rx Failed Frame Count................... 0

Rate Limiting Stats:
  Wlan 1:
    Number of Data Packets Received.............. 592
    Number of Data Rx Packets Dropped............ 160
    Number of Data Bytes Received................ 160783
    Number of Data Rx Bytes Dropped.............. 0
    Number of Realtime Packets Received.......... 592
    Number of Realtime Rx Packets Dropped........ 0
    Number of Realtime Bytes Received............ 160783
    Number of Realtime Rx Bytes Dropped.......... 0
    Number of Data Packets Sent.................. 131
    Number of Data Tx Packets Dropped............ 0
    Number of Data Bytes Sent.................... 23436
    Number of Data Tx Bytes Dropped.............. 0
    Number of Realtime Packets Sent.............. 131
    Number of Realtime Tx Packets Dropped........ 0
    Number of Realtime Bytes Sent................ 23436
    Number of Realtime Tx Bytes Dropped.......... 0
Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw)......... 0
  Voice Roam Bandwidth in use(% of config bw).... 0
    Total channel MT free....................... 0
    Total voice MT free......................... 0
    Na Direct................................... 0
```

```
    Na Roam..................................... 0
  Video Bandwidth in use(% of config bw)........ 0
  Video Roam Bandwidth in use(% of config bw).... 0
  Total BW in use for Voice(%)................... 0
  Total BW in use for SIP Preferred call(%)...... 0
WMM TSPEC CAC Call Stats
  Total num of voice calls in progress........... 0
  Num of roaming voice calls in progress......... 0
  Total Num of voice calls since AP joined....... 0
  Total Num of roaming calls since AP joined..... 0
  Total Num of exp bw requests received.......... 0
  Total Num of exp bw requests admitted.......... 0
  Num of voice calls rejected since AP joined.... 0
  Num of roam calls rejected since AP joined..... 0
  Num of calls rejected due to 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 roaming calls in progress............... 0
  Total Num of calls since AP joined............. 0
  Total Num of roaming calls since AP joined..... 0
  Total Num of Preferred calls received.......... 0
  Total Num of Preferred calls accepted.......... 0
  Total Num of ongoing Preferred calls........... 0
  Total Num of calls rejected(Insuff BW)......... 0
  Total Num of roam calls rejected(Insuff BW).... 0
WMM Video TSPEC CAC Call Stats
  Total num of video calls in progress........... 0
  Num of roaming video calls in progress......... 0
  Total Num of video calls since AP joined....... 0
  Total Num of video roaming calls since AP j.... 0
  Num of video calls rejected since AP joined.... 0
  Num of video roam calls rejected since AP j.... 0
  Num of video calls rejected due to insuffic.... 0
  Num of video calls rejected due to invalid .... 0
  Num of video calls rejected due to PHY rate.... 0
  Num of video calls rejected due to QoS poli.... 0
SIP Video CAC Call Stats
  Total Num of video calls in progress........... 0
  Num of video roaming calls in progress......... 0
  Total Num of video calls since AP joined....... 0
  Total Num of video roaming calls since AP j.... 0
  Total Num of video calls rejected(Insuff BW.... 0
  Total Num of video roam calls rejected(Insu.... 0
Band Select Stats
  Num of dual band client ....................... 0
  Num of dual band client added.................. 0
  Num of dual band client expired ............... 0
  Num of dual band client replaced............... 0
  Num of dual band client detected .............. 0
  Num of suppressed client ...................... 0
  Num of suppressed client expired............... 0
  Num of suppressed client replaced.............. 0
```

show ap summary

To display a summary of all lightweight access points attached to the controller, use the **show ap summary** command.

show ap summary [*cisco_ap*]

Syntax Description

cisco_ap	(Optional) Type sequence of characters that make up the name of a specific AP or a group of APs, or enter a wild character search pattern.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

A list that contains each lightweight access point name, number of slots, manufacturer, MAC address, location, and the controller port number appears. When you specify

The following example shows how to display a summary of all connected access points:

```
(Cisco Controller) >show ap summary
Number of APs.................................... 2
Global AP username............................... user
Global AP Dot1x username......................... Not Configured
Number of APs.................................... 2
Global AP username............................... user
Global AP Dot1x username......................... Not Configured


 AP Name             Slots  AP Model              Ethernet MAC       Location
Country  IP Address       Clients
------------------  -----  --------------------  -----------------  ----------------  -------
  ---------------  -------
AP1140               2     AIR-LAP1142N-A-K9     f0:f7:55:75:f3:29               default
location         US   192.168.0.0         0
Access Points using IPv6 transport:
 AP Name    Slots   AP Model           Ethernet MAC       Location         Country     IPv6
 Address                Clients
 ------------------ ----- ---------------------------------- ------------
------------------ ----- ---------------------------- ------
 AP1040      2    AIR-LAP1042N-A-K9   00:40:96:b9:4b:89   default location  US
2001:DB8:0:1::1                   0
```

show ap tcp-mss-adjust

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point, use the **show ap tcp-mss-adjust** command.

show ap tcp-mss-adjust {*cisco_ap* | **all**}

Syntax Description

cisco_ap	Specified lightweight access point name.
all	Specifies all access points.

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

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display Transmission Control Protocol (TCP) maximum segment size (MSS) information of all access points:

```
(Cisco Controller) >show ap tcp-mss-adjust all
AP Name            TCP State MSS Size
------------------ --------- -------
AP-1140            enabled   536
AP-1240            disabled  -
AP-1130            disabled  -
```

show ap wlan

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point, use the **show ap wlan** command.

show ap wlan 802.11{**a** | **b**} *cisco_ap*

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
ap_name	Lightweight access point name.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display BSSIDs of an access point for the 802.11b network:

```
(Cisco Controller) >show ap wlan 802.11b AP01
Site Name..................................... MY_AP_GROUP1
Site Description.............................. MY_AP_GROUP1
WLAN ID          Interface          BSSID
-------         -----------        --------------------------
1               management           00:1c:0f:81:fc:20
2               dynamic              00:1c:0f:81:fc:21
```

show auth-list

To display the access point authorization list, use the **show auth-list** command.

show auth-list

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the access point authorization list:

```
(Cisco Controller) >show auth-list
Authorize APs against AAA..................... disabled
Allow APs with Self-signed Certificate (SSC)... disabled
Mac Addr                  Cert Type    Key Hash
-----------------------   ----------   ----------------------------------------
xx:xx:xx:xx:xx:xx         MIC
```

show client ap

To display the clients on a Cisco lightweight access point, use the **show client ap** command.

show client ap 802.11{**a** | **b**} *cisco_ap*

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Usage Guidelines

The **show client ap** command may list the status of automatically disabled clients. Use the **show exclusionlist** command to view clients on the exclusion list.

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to display client information on an access point:

```
(Cisco Controller) >show client ap 802.11b AP1
MAC Address        AP Id   Status         WLAN Id    Authenticated
-----------------  ------  -------------  ---------  -------------
xx:xx:xx:xx:xx:xx      1   Associated     1          No
```

show boot

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

show boot

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

Related Commands

config boot

show country

To display the configured country and the radio types that are supported, use the **show country** command.

show country

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the configured countries and supported radio types:

```
(Cisco Controller) >show country
Configured Country..............................  United States
Configured Country Codes
US  - United States.............................  802.11a / 802.11b / 802.11g
```

show country channels

To display the radio channels supported in the configured country, use the **show country channels** command.

show country channels

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the auto-RF channels for the configured countries:

```
(Cisco Controller) >show country channels
Configured Country..............................  United States
      KEY: * = Channel is legal in this country and may be configured manually.
Configured Country..............................  United States
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11BG :
Channels :                   1 1 1 1 1
         : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
     US  : A * * * * A * * * * A . . .
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A :  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
         : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
     US  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

show country supported

To display a list of the supported country options, use the **show country supported** command.

show country supported

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a list of all the supported countries:

```
(Cisco Controller) >show country supported
Configured Country..................................... United States
Supported Country Codes
AR  - Argentina................................... 802.11a / 802.11b / 802.11g
AT  - Austria..................................... 802.11a / 802.11b / 802.11g
AU  - Australia................................... 802.11a / 802.11b / 802.11g
BR  - Brazil...................................... 802.11a / 802.11b / 802.11g
BE  - Belgium..................................... 802.11a / 802.11b / 802.11g
BG  - Bulgaria.................................... 802.11a / 802.11b / 802.11g
CA  - Canada...................................... 802.11a / 802.11b / 802.11g
CH  - Switzerland................................. 802.11a / 802.11b / 802.11g
CL  - Chile.......................................           802.11b / 802.11g
CN  - China....................................... 802.11a / 802.11b / 802.11g
CO  - Colombia....................................           802.11b / 802.11g
CY  - Cyprus...................................... 802.11a / 802.11b / 802.11g
CZ  - Czech Republic.............................. 802.11a / 802.11b
DE  - Germany..................................... 802.11a / 802.11b / 802.11g
DK  - Denmark..................................... 802.11a / 802.11b / 802.11g
EE  - Estonia..................................... 802.11a / 802.11b / 802.11g
ES  - Spain....................................... 802.11a / 802.11b / 802.11g
FI  - Finland..................................... 802.11a / 802.11b / 802.11g
FR  - France...................................... 802.11a / 802.11b / 802.11g
GB  - United Kingdom.............................. 802.11a / 802.11b / 802.11g
GI  - Gibraltar................................... 802.11a / 802.11b / 802.11g
GR  - Greece...................................... 802.11a / 802.11b / 802.11g
HK  - Hong Kong................................... 802.11a / 802.11b / 802.11g
HU  - Hungary..................................... 802.11a / 802.11b / 802.11g
ID  - Indonesia...................................           802.11b / 802.11g
IE  - Ireland..................................... 802.11a / 802.11b / 802.11g
IN  - India....................................... 802.11a / 802.11b / 802.11g
IL  - Israel...................................... 802.11a / 802.11b / 802.11g
ILO - Israel (outdoor).............................           802.11b / 802.11g
IS  - Iceland..................................... 802.11a / 802.11b / 802.11g
IT  - Italy....................................... 802.11a / 802.11b / 802.11g
JP  - Japan (J)................................... 802.11a / 802.11b / 802.11g
J2  - Japan 2(P).................................. 802.11a / 802.11b / 802.11g
J3  - Japan 3(U).................................. 802.11a / 802.11b / 802.11g
KR  - Korea Republic (C).......................... 802.11a / 802.11b / 802.11g
KE  - Korea Extended (K).......................... 802.11a / 802.11b / 802.11g
LI  - Liechtenstein............................... 802.11a / 802.11b / 802.11g
LT  - Lithuania................................... 802.11a / 802.11b / 802.11g
LU  - Luxembourg.................................. 802.11a / 802.11b / 802.11g
```

```
LV  - Latvia..................................... 802.11a / 802.11b / 802.11g
MC  - Monaco..................................... 802.11a / 802.11b / 802.11g
MT  - Malta...................................... 802.11a / 802.11b / 802.11g
MX  - Mexico..................................... 802.11a / 802.11b / 802.11g
MY  - Malaysia................................... 802.11a / 802.11b / 802.11g
NL  - Netherlands................................ 802.11a / 802.11b / 802.11g
NZ  - New Zealand................................ 802.11a / 802.11b / 802.11g
NO  - Norway..................................... 802.11a / 802.11b / 802.11g
PA  - Panama.....................................           802.11b / 802.11g
PE  - Peru.......................................           802.11b / 802.11g
PH  - Philippines................................ 802.11a / 802.11b / 802.11g
PL  - Poland..................................... 802.11a / 802.11b / 802.11g
PT  - Portugal................................... 802.11a / 802.11b / 802.11g
RU  - Russian Federation......................... 802.11a / 802.11b / 802.11g
RO  - Romania.................................... 802.11a / 802.11b / 802.11g
SA  - Saudi Arabia............................... 802.11a / 802.11b / 802.11g
SE  - Sweden..................................... 802.11a / 802.11b / 802.11g
SG  - Singapore.................................. 802.11a / 802.11b / 802.11g
SI  - Slovenia................................... 802.11a / 802.11b / 802.11g
SK  - Slovak Republic............................ 802.11a / 802.11b / 802.11g
TH  - Thailand...................................           802.11b / 802.11g
TR  - Turkey.....................................           802.11b / 802.11g
TW  - Taiwan..................................... 802.11a / 802.11b / 802.11g
UA  - Ukraine.................................... 802.11a / 802.11b / 802.11g
US  - United States.............................. 802.11a / 802.11b / 802.11g
USL - United States (Legacy)..................... 802.11a / 802.11b / 802.11g
USX - United States (US + chan165)............... 802.11a / 802.11b / 802.11g
VE  - Venezuela..................................           802.11b / 802.11g
ZA  - South Africa............................... 802.11a / 802.11b / 802.11g
```

show dtls connections

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

show dtls connections

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

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

```
Device > show dtls connections

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

show known ap

To display known Cisco lightweight access point information, use the **show known ap** command.

show known ap {**summary** | **detailed** *MAC*}

Syntax Description

summary	Displays a list of all known access points.
detailed	Provides detailed information for all known access points.
MAC	MAC address of the known AP.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a summary of all known access points:

```
(Cisco Controller) >show known ap summary
MAC Address         State        # APs  # Clients   Last Heard
-----------         -----------  -----   --------   -----------------
```

show msglog

To display the message logs written to the controller database, use the **show msglog** command.

show msglog

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

If there are more that 15 entries, you are prompted to display the messages shown in the example.

The following example shows how to display message logs:

```
 (Cisco Controller) >show msglog
Message Log Severity Level..................... ERROR
Thu Aug  4 14:30:08 2005  [ERROR] spam_lrad.c 1540: AP 00:0b:85:18:b6:50 associated. Last
AP failure was due to Link Failure
Thu Aug  4 14:30:08 2005  [ERROR] spam_lrad.c 13840: Updating IP info for AP 00:
0b:85:18:b6:50 -- static 0, 1.100.49.240/255.255.255.0, gtw 1.100.49.1
Thu Aug  4 14:29:32 2005  [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Thu Aug  4 14:29:32 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11a switch group
reset
Thu Aug  4 14:29:32 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Thu Aug  4 14:29:22 2005  [ERROR] sim.c 2841: Unable to get link state for primary port 0
of interface ap-manager
Thu Aug  4 14:29:22 2005  [ERROR] dtl_l2_dot1q.c 767: Unable to get USP
Thu Aug  4 14:29:22 2005  Previous message occurred 2 times
Thu Aug  4 14:29:14 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake called with
NULL pointer: osapi_bsntime.c:927
Thu Aug  4 14:29:14 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake called with
NULL pointer: osapi_bsntime.c:919
Thu Aug  4 14:29:14 2005  [CRITICAL] hwutils.c 1861: Security Module not found
Thu Aug  4 14:29:13 2005  [CRITICAL] bootos.c 791: Starting code...
```

show network summary

To display the network configuration of the Cisco wireless LAN controller, use the **show network summary** command.

show network summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to display a summary configuration:

```
(Cisco Controller) >show network summary
RF-Network Name............................. RF
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
Secure Web Mode RC4 Cipher Preference....... Disable
OCSP........................................ Disabled
OCSP responder URL..........................
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable   Mode: Ucast
Ethernet Broadcast Mode..................... Disable
Ethernet Multicast Forwarding............... Disable
Ethernet Broadcast Forwarding............... Disable
AP Multicast/Broadcast Mode................. Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
IGMP Query Interval......................... 20 seconds
MLD snooping................................ Disabled
MLD timeout................................. 60 seconds
MLD query interval.......................... 20 seconds
User Idle Timeout........................... 300 seconds
AP Join Priority............................ Disable
ARP Idle Timeout............................ 300 seconds
ARP Unicast Mode............................ Disabled
Cisco AP Default Master..................... Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Over The Air Provisioning of AP's........... Enable
Apple Talk ................................. Disable
Mesh Full Sector DFS........................ Enable
AP Fallback ................................ Disable
Web Auth CMCC Support ...................... Disabled
Web Auth Redirect Ports .................... 80
Web Auth Proxy Redirect  ................... Disable
Web Auth Captive-Bypass   .................. Disable
Web Auth Secure Web  ....................... Enable
```

```
Fast SSID Change ........................... Disabled
AP Discovery - NAT IP Only ................. Enabled
IP/MAC Addr Binding Check .................. Enabled
CCX-lite status ............................ Disable
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 watchlist

To display the client watchlist, use the **show watchlist** command.

show watchlist

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the client watchlist information:

```
(Cisco Controller) >show watchlist
client watchlist state is disabled
```

RRM Commands

show Commands

This section lists the **show** commands to display information about your Radio Resource Management (RRM) configuration settings.

show 802.11 extended

To display access point radio extended configurations, use the **show 802.11 extended** command.

show 802.11 {**a** | **b**} **extended**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
extended	Displays the 802.11a/b radio extended configurations.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display radio extended configurations:

```
(Cisco Controller) > show 802.11a extended
Default 802.11a band radio extended configurations:
    beacon period 300, range 60;
    multicast buffer 45, rate 200;
    RX SOP -80; CCA threshold -90;
AP0022.9090.b618 00:24:97:88:99:60
    beacon period 300, range 60; multicast buffer 45, rate 200;
    RX SOP -80; CCA threshold -77
AP0022.9090.bb3e 00:24:97:88:c5:d0
    beacon period 300, range 0; multicast buffer 0, rate 0;
    RX SOP -80; CCA threshold -0
ironRap.ddbf 00:17:df:36:dd:b0
    beacon period 300, range 0; multicast buffer 0, rate 0;
    RX SOP  -80; CCA threshold -0
```

The following example shows how to display radio extended configurations and the Rx SOP threshold:

```
(Cisco Controller) > show 802.11a extended
Default 802.11a band Radio Extended Configurations:
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: -76; CCA threshold: 0 (AUTO);

AP3600-XALE3  34:a8:4e:6a:7b:00
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: -76; CCA threshold: 0 (AUTO);
```

show advanced 802.11 channel

To display the automatic channel assignment configuration and statistics, use the **show advanced 802.11 channel** command.

show advanced 802.11{**a** | **b**} **channel**

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the automatic channel assignment configuration and statistics:

```
(Cisco Controller) > show advanced 802.11a channel
Automatic Channel Assignment
  Channel Assignment Mode..................... AUTO
  Channel Update Interval..................... 600 seconds [startup]
  Anchor time (Hour of the day)............... 0
  Channel Update Contribution................. SNI.
  Channel Assignment Leader................... 00:1a:6d:dd:1e:40
  Last Run.................................... 129 seconds ago
  DCA Sensitivity Level: ..................... STARTUP (5 dB)
  DCA Minimum Energy Limit.................... -95 dBm
Channel Energy Levels
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Channel Dwell Times
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Auto-RF Allowed Channel List...............
36,40,44,48,52,56,60,64,149,
    ............................................ 153,157,161
  Auto-RF Unused Channel List................
100,104,108,112,116,132,136,
    ............................................ 140,165,190,196
  DCA Outdoor AP option....................... Enabled
```

show advanced 802.11 coverage

To display the configuration and statistics for coverage hole detection, use the **show advanced 802.11 coverage** command.

show advanced 802.11 {**a** | **b**} **coverage**

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the statistics for coverage hole detection:

```
(Cisco Controller) > show advanced 802.11a coverage
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode.......... Enabled
  802.11a Coverage Voice Packet Count........... 100 packets
  802.11a Coverage Voice Packet Percentage...... 50%
  802.11a Coverage Voice RSSI Threshold......... -80 dBm
  802.11a Coverage Data Packet Count............ 50 packets
  802.11a Coverage Data Packet Percentage....... 50%
  802.11a Coverage Data RSSI Threshold.......... -80 dBm
  802.11a Global coverage exception level....... 25 %
  802.11a Global client minimum exception lev.... 3 clients
```

Related Topics

config advanced 802.11 coverage exception global, on page 716
config advanced 802.11 coverage fail-rate, on page 717
config advanced 802.11 coverage level global, on page 718
config advanced 802.11 coverage packet-count, on page 718
config advanced 802.11 coverage rssi-threshold, on page 719
config advanced 802.11 edca-parameters, on page 88

show advanced 802.11 group

To display 802.11a or 802.11b Cisco radio RF grouping, use the **show advanced 802.11 group** command.

show advanced 802.11 {**a** | **b**} **group**

Syntax Description

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

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display Cisco radio RF group settings:

```
(Cisco Controller) > show advanced 802.11a group
Radio RF Grouping
  802.11a Group Mode..................................... AUTO
  802.11a Group Update Interval.......................... 600 seconds
  802.11a Group Leader................................... xx:xx:xx:xx:xx:xx
    802.11a Group Member................................. xx:xx:xx:xx:xx:xx
  802.11a Last Run....................................... 133 seconds ago
```

Related Topics

config advanced 802.11 group-mode, on page 724

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 802.11 logging

To display 802.11a or 802.11b RF event and performance logging, use the **show advanced 802.11 logging** command.

show advanced 802.11{a | b} logging

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display 802.11b RF event and performance logging:

```
(Cisco Controller) > show advanced 802.11b logging
RF Event and Performance Logging
  Channel Update Logging..................... Off
  Coverage Profile Logging................... Off
  Foreign Profile Logging.................... Off
  Load Profile Logging....................... Off
  Noise Profile Logging...................... Off
  Performance Profile Logging................ Off
  TxPower Update Logging..................... Off
```

Related Topics

config advanced 802.11 logging channel, on page 725
config advanced 802.11 logging coverage, on page 725
config advanced 802.11 logging foreign, on page 726
config advanced 802.11 logging load, on page 727
config advanced 802.11 logging noise, on page 727
config advanced 802.11 logging performance, on page 728

show advanced 802.11 monitor

To display the 802.11a or 802.11b default Cisco radio monitoring, use the **show advanced 802.11 monitor** command.

show advanced 802.11{a | b} monitor

Syntax Description

a	Specifies the 802.11a network.

b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the radio monitoring for the 802.11b network:

```
(Cisco Controller) > show advanced 802.11b monitor
Default 802.11b AP monitoring
  802.11b Monitor Mode.......................... enable
  802.11b Monitor Channels...................... Country channels
  802.11b RRM Neighbor Discovery Type........... Transparent
  802.11b AP Coverage Interval.................. 180 seconds
  802.11b AP Load Interval...................... 60 seconds
  802.11b AP Noise Interval..................... 180 seconds
  802.11b AP Signal Strength Interval........... 60 seconds
```

Related Topics

config advanced 802.11 monitor load, on page 731
config advanced 802.11 monitor mode, on page 731
config advanced 802.11 monitor noise, on page 733
config advanced 802.11 monitor signal, on page 733

show advanced 802.11 optimized roaming

To display the optimized roaming configurations for 802.11a/b networks, use the **show advanced 802.11 optimized roaming** command.

show advanced 802.11 {**a** | **b**} **optimized roaming** [**stats**]

Syntax Description

stats	(Optional) Displays optimized roaming statistics for a 802.11a/b network.

Command Default

None

Command History

Release	Modification
8.8	This command was introduced.

The following example shows how to display the optimized roaming configurations for an 802.11a network:

```
(Cisco Controller) > show advanced 802.11a optimized roaming
OptimizedRoaming
  802.11a OptimizedRoaming Mode................. Enabled
  802.11a OptimizedRoaming Reporting Interval.... 20 seconds
  802.11a OptimizedRoaming Rate Threshold........ disabled
```

The following example shows how to display the optimized roaming statistics for an 802.11a network:

```
(Cisco Controller) > show advanced 802.11a optimized roaming stats
OptimizedRoaming Stats
802.11a OptimizedRoaming Disassociations....... 2
802.11a OptimizedRoaming Rejections............ 1
```

Related Topics

config advanced 802.11 optimized roaming, on page 734

show advanced 802.11 profile

To display the 802.11a or 802.11b lightweight access point performance profiles, use the **show advanced 802.11 profile** command.

show advanced 802.11{**a** | **b**} **profile** {**global** | *cisco_ap*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Specifies all Cisco lightweight access points.
cisco_ap	Name of a specific Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the global configuration and statistics of an 802.11a profile:

```
(Cisco Controller) > show advanced 802.11 profile global
Default 802.11a AP performance profiles
  802.11a Global Interference threshold.............. 10%
  802.11a Global noise threshold..................... -70 dBm
  802.11a Global RF utilization threshold............ 80%
  802.11a Global throughput threshold................ 1000000 bps
  802.11a Global clients threshold................... 12 clients
  802.11a Global coverage threshold.................. 12 dB
  802.11a Global coverage exception level............ 80%
  802.11a Global client minimum exception lev........ 3 clients
```

The following example shows how to display the configuration and statistics of a specific access point profile:

```
(Cisco Controller) >  show advanced 802.11 profile AP1
```

```
Cisco AP performance profile not customized
```

This response indicates that the performance profile for this lightweight access point is using the global defaults and has not been individually configured.

Related Topics

config advanced 802.11 profile noise, on page 542
config advanced 802.11 profile foreign, on page 541

show advanced 802.11 receiver

To display the configuration and statistics of the 802.11a or 802.11b receiver, use the **show advanced 802.11 receiver** command.

show advanced 802.11{**a** | **b**} **receiver**

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the configuration and statistics of the 802.11a network settings:

```
(Cisco Controller) > show advanced 802.11 receiver
802.11a Receiver Settings
  RxStart    : Signal Threshold.......................... 15
  RxStart    : Signal Lamp Threshold..................... 5
  RxStart    : Preamble Power Threshold.................. 2
  RxReStart : Signal Jump Status........................ Enabled
  RxReStart : Signal Jump Threshold..................... 10
  TxStomp : Low RSSI Status............................. Enabled
  TxStomp : Low RSSI Threshold.......................... 30
  TxStomp : Wrong BSSID Status.......................... Enabled
  TxStomp : Wrong BSSID Data Only Status................ Enabled
  RxAbort : Raw Power Drop Status....................... Disabled
  RxAbort : Raw Power Drop Threshold.................... 10
  RxAbort : Low RSSI Status............................. Disabled
  RxAbort : Low RSSI Threshold.......................... 0
  RxAbort : Wrong BSSID Status.......................... Disabled
  RxAbort : Wrong BSSID Data Only Status................ Disabled
```

show advanced 802.11 summary

To display the 802.11a or 802.11b Cisco lightweight access point name, channel, and transmit level summary, use the **show advanced 802.11 summary** command.

show advanced 802.11 {**a** | **b**} **summary**

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display a summary of the 802.11b access point settings:

```
(Cisco Controller) > show advanced 802.11b summary
AP Name       MAC Address         Admin State  Operation State   Channel
TxPower
------------ ------------------ ------------ ----------------- -------
--------
CJ-1240       00:21:1b:ea:36:60    ENABLED          UP            161
 1( )
CJ-1130       00:1f:ca:cf:b6:60    ENABLED          UP            56*
 1(*)
```

Note An asterisk (*) next to a channel number or power level indicates that it is being controlled by the global algorithm settings.

Related Topics

config advanced 802.11 7920VSIEConfig, on page 88
config advanced 802.11 channel add, on page 706

show advanced 802.11 txpower

To display the 802.11a or 802.11b automatic transmit power assignment, use the **show advanced 802.11 txpower** command.

show advanced 802.11 {**a** | **b**} **txpower**

Syntax Description

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

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the configuration and statistics of the 802.11b transmit power cost:

```
(Cisco Controller) > show advanced 802.11b txpower
Automatic Transmit Power Assignment
  Transmit Power Assignment Mode.................. AUTO
  Transmit Power Update Interval.................. 600 seconds
  Transmit Power Threshold........................ -65 dBm
  Transmit Power Neighbor Count................... 3 APs
  Transmit Power Update Contribution.............. SN.
  Transmit Power Assignment Leader................ xx:xx:xx:xx:xx:xx
  Last Run........................................ 384 seconds ago
```

Related Topics

config 802.11 txPower, on page 704

show advanced dot11-padding

To display the state of over-the-air frame padding on a wireless LAN controller, use the **show advanced dot11-padding** command.

show advanced dot11-padding

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 view the state of over-the-air frame padding:

```
(Cisco Controller) > show advanced dot11-padding
dot11-padding................................... Disabled
```

Related Topics

config advanced dot11-padding, on page 547
debug dot11, on page 749

show client location-calibration summary

To display client location calibration summary information, use the **show client location-calibration summary** command.

show client location-calibration summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the location calibration summary information:

```
(Cisco Controller) >show client location-calibration summary
MAC Address Interval
----------- ----------
10:10:10:10:10:10 60
21:21:21:21:21:21 45
```

config Commands

This section lists the **config** commands to configure Radio Resource Management (RRM).

config 802.11-a

To enable or disable the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a** command.

config {**802.11-a49** | **802.11-a58**} {**enable** | **disable**} *cisco_ap*

Syntax Description

802.11-a49	Specifies the 4.9-GHz public safety channel.
802.11-a58	Specifies the 5.8-GHz public safety channel.
enable	Enables the use of this frequency on the designated access point.
disable	Disables the use of this frequency on the designated access point.
cisco_ap	Name of the access point to which the command applies.

Command Default

The default 4.9-GHz and 5.8-GHz public safety channels on an access point is disabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the 4.9-GHz public safety channel on ap_24 access point:

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

Related Topics

config 802.11-a antenna extAntGain, on page 530
config 802.11-a channel ap, on page 531
config 802.11-a txpower ap, on page 532

config 802.11-a antenna extAntGain

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

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

Syntax Description

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

Command Default

Channel properties are disabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

Related Topics

config 802.11-a channel ap, on page 531

config 802.11-a channel ap

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

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

Syntax Description

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

Command Default

Channel properties are disabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to set the channel properties:

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

Related Topics

config 802.11-a antenna extAntGain, on page 530
config 802.11-a, on page 685

config 802.11-a txpower ap

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

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

Syntax Description

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

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

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

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

Related Topics

config 802.11-a antenna extAntGain, on page 530

config 802.11-a, on page 685
config 802.11-a channel ap, on page 531

config 802.11-abgn

To configure dual-band radio parameters on an access point, use the **config 802.11-abgn** command.

config 802.11-abgn {**cleanair** {**enable** | **disable**} {*cisco_ap* **band** *band*} | {**enable** | **disable**} {*cisco_ap*}}

Syntax Description

cleanair	Configures CleanAir on the dual-band radio.
enable	Enables CleanAir for both 2.4-GHz and 5-GHz radios.
disable	Disables CleanAir for both 2.4-GHz and 5-GHz radios.
cisco_ap	Name of the access point to which the command applies.
band	Configures the radio band.
band	Radio band that can be 2.4-GHz or 5-GHz.
enable	Enables the dual-band radio on an access point.
disable	Disables the dual-band radio on an access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

The following example shows how to enable Cisco CleanAir on an access point:

```
(Cisco Controller) >config 802.11-abgn cleanair enable AP3600 band 5
```

Related Topics

config 802.11-a, on page 685

config 802.11a 11acsupport

To configure 802.11ac 5-GHz parameters, use the **config 802.11a 11acsupport**

config 802.11a 11acsupport {**enable** | **disable** | **mcs tx** *mcs_index* **ss** *spatial_stream* {**enable** | **disable**}}

Syntax Description

enable	Enables 802.11ac 5-GHz mode.
disable	Disables 802.11ac 5-GHz mode.
mcs tx	Configures 802.11ac 5-GHz Modulation and Coding Scheme (MCS) rates at which data can be transmitted between the access point and the client.
tx	Configures 802.11ac 5-GHz MCS transmit rates.
mcs_index	MCS index value of 8 or 9. MCS data rates with index 8 or 9 are specific to 802.11ac. When you enable an MCS data rate with index 9, the data rate with MCS index 8 is automatically enabled.
ss	Configures the 802.11ac 5-GHz MCS spatial stream (SS).
spatial_stream	Spatial stream within which you can enable or disable an MCS data rate. Signals transmitted by the various antennae are multiplexed by using different spaces within the same spectral channel. These spaces are known as spatial streams. Three spatial streams are available within which you can enable or disable a MCS rate. The range is from 1 to 3.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Disabling the 802.11n/ac mode applies only to access radios. Backhaul radios always have 802.11n/ac mode enabled if they are 802.11n capable.

The following example shows how to configure the MCS index for spatial stream 3:

```
(Cisco Controller) >config 802.11a 11acsupport mcs tx 9 ss 3
```

Related Topics

config 802.11 11nsupport, on page 52
config 802.11 chan_width, on page 702
config 802.11 channel ap, on page 701

config 802.11b 11gSupport

To enable or disable the Cisco wireless LAN solution 802.11g network, use the **config 802.11b 11gSupport** command.

config 802.11b 11gSupport {**enable** | **disable**}

Syntax Description

enable	Enables the 802.11g network.

disable	Disables the 802.11g network.

Command Default

The default network for Cisco wireless LAN solution 802.11g is enabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Before you enter the **config 802.11b 11gSupport** {**enable** | **disable**} command, disable the 802.11 Cisco radio with the **config 802.11 disable** command.

After you configure the support for the 802.11g network, use the **config 802.11 enable** command to enable the 802.11 radio.

Note To disable an 802.11a, 802.11b and/or 802.11g network for an individual wireless LAN, use the **config wlan radio** command.

The following example shows how to enable the 802.11g network:

```
(Cisco Controller) > config 802.11b 11gSupport enable
Changing the 11gSupport will cause all the APs to reboot when you enable
 802.11b network.
Are you sure you want to continue? (y/n) n
11gSupport not changed!
```

Related Topics

config 802.11-a, on page 685

config 802.11b preamble

To change the 802.11b preamble as defined in subclause 18.2.2.2 to **long** (slower, but more reliable) or **short** (faster, but less reliable), use the **config 802.11b preamble** command.

config 802.11b preamble {**long** | **short**}

Syntax Description

long	Specifies the long 802.11b preamble.
short	Specifies the short 802.11b preamble.

Command Default

The default 802.11b preamble value is short.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Note You must reboot the Cisco Wireless LAN Controller (reset system) with save to implement this command.

This parameter must be set to **long** to optimize this Cisco wireless LAN controller for some clients, including SpectraLink NetLink telephones.

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

The following example shows how to change the 802.11b preamble to short:

```
(Cisco Controller) >config 802.11b preamble short
(Cisco Controller) >(reset system with save)
```

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 channe
quiet	Enables 802.11h-enabled clients to stop transmitting packets immediate 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

Usage Guidelines

Cisco Catalyst 9120AXE, 9120AXP, and Cisco Catalyst 9130AXE access points should have at least two antennas configured if you want to disable this configuration.

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, on page 685

config 802.11 antenna diversity

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the diversity.
sideA	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point left port.
sideB	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point right port.
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 enable antenna diversity for AP01 on an 802.11b network:

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

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

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

Related Topics

config 802.11-a, on page 685

config 802.11 antenna extAntGain

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

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

Syntax Description

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

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

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

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

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

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

Related Topics

config 802.11-a, on page 685

config 802.11 antenna mode

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
omni	Specifies to use both internal antennas.
sectorA	Specifies to use only the side A internal antenna.
sectorB	Specifies to use only the side B internal antenna.
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 access point AP01 antennas for a 360-degree omnidirectional pattern on an 802.11b network:

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

Related Topics

config 802.11-a, on page 685

config 802.11 antenna selection

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
internal	Specifies the internal antenna.
external	Specifies the external antenna.
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 access point AP02 on an 802.11b network to use the internal antenna:

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

Related Topics

config 802.11-a, on page 685

config 802.11 channel

To configure an 802.11 network or a single access point for automatic or manual channel selection, use the **config 802.11 channel** command.

config 802.11 {**a** | **b**} **channel** {**global** [**auto** | **once** | **off** | **restart**]} | **ap** {*ap_name* [**global** | *channel*]}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Specifies the 802.11a operating channel that is automatically set by RRM and overrides the existing configuration setting.
auto	(Optional) Specifies that the channel is automatically set by Radio Resource Management (RRM) for the 802.11a radio.
once	(Optional) Specifies that the channel is automatically set once by RRM.
off	(Optional) Specifies that the automatic channel selection by RRM is disabled.
restarts	(Optional) Restarts the aggressive DCA cycle.
ap_name	Access point name.
channel	Manual channel number to be used by the access point. The supported channels depend on the specific access point used and the regulatory region.

Command Default None

Usage Guidelines When configuring 802.11 channels for a single lightweight access point, enter the **config 802.11 disable** command to disable the 802.11 network. Enter the **config 802.11 channel** command to set automatic channel selection by Radio Resource Management (RRM) or manually set the channel for the 802.11 radio, and enter the **config 802.11 enable** command to enable the 802.11 network.

Note See the Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points document for the channels supported by your access point. The power levels and available channels are defined by the country code setting and are regulated on a country-by-country basis.

The following example shows how to have RRM automatically configure the 802.11a channels for automatic channel configuration based on the availability and interference:

```
(Cisco Controller) >config 802.11a channel global auto
```

The following example shows how to configure the 802.11b channels one time based on the availability and interference:

```
(Cisco Controller) >config 802.11b channel global once
```

The following example shows how to turn 802.11a automatic channel configuration off:

```
(Cisco Controller) >config 802.11a channel global off
```

The following example shows how to configure the 802.11b channels in access point AP01 for automatic channel configuration:

```
(Cisco Controller) >config 802.11b AP01 channel global
```

The following example shows how to configure the 802.11a channel 36 in access point AP01 as the default channel:

```
(Cisco Controller) >config 802.11a channel AP01 36
```

Related Topics

config 802.11-a, on page 685

config 802.11 channel ap

To set the operating radio channel for an access point, use the **config 802.11 channel ap** command.

config 802.11 {**a** | **b**} **channel ap** *cisco_ap* {**global** | *channel_no*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
cisco_ap	Name of the Cisco access point.
global	Enables auto-RF on the designated access point.
channel_no	Default channel from 1 to 26, inclusive.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable auto-RF for access point AP01 on an 802.11b network:

```
(Cisco Controller) >config 802.11b channel ap AP01 global
```

Related Topics

config 802.11-a, on page 685

config 802.11 chan_width

To configure the channel width for a particular access point, use the **config 802.11 chan_width** command.

config 802.11{**a** | **b**} **chan_width** *cisco_ap* {**20** | **40** | **80** | **160** | **best**}

Syntax Description

a	Configures the 802.11a radio on slot 1 and 802.11ac/ax radio on slot 2.
b	Specifies the 802.11b/g radio.
cisco_ap	Access point.
20	Allows the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels.
40	Allows 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together.
80	Allows 80-MHz 802.11ac/ax radios to communicate using two adjacent 40-MHz channels bonded together.
160	Allows 160-MHz 802.11ac/ax radios to communicate.
best	In this mode, the device selects the optimum bandwidth channel.

Command Default

The default channel width is 20.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

This parameter can be configured only if the primary channel is statically assigned.

Caution We recommend that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference can occur.

Statically configuring an access point's radio for 20-MHz or 40-MHz mode overrides the globally configured DCA channel width setting (configured by using the **config advanced 802.11 channel dca chan-width** command). If you change the static configuration back to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

The following example shows how to configure the channel width for access point AP01 on an 802.11 network using 40-MHz channels:

```
(Cisco Controller) >config 802.11a chan_width AP01 40
```

Related Topics

config 802.11-a, on page 685

config 802.11 rx-sop threshold

To configure the threshold values for Receiver Start of Packet Detection Threshold (RxSOP) for each 802.11 band, use the **config 802.11 rx-sop threshold** command.

config {**802.11a | 802.11b** } **rx-sop threshold** {**high | low | medium | default** |*custom_value*} **ap** *ap_name*

Syntax Description

802.11a	Configures an RxSOP threshold value for the 802.11a network.
802.11b	Configures an RxSOP threshold value for the 802.11b network.
high	Configures the high RxSOP threshold value for 802.11a/b networks.
medium	Configures the medium RxSOP threshold value for 802.11a/b networks.
low	Configures the low RxSOP threshold value for 802.11a/b networks.
ap *ap_name*	Configures the RxSOP threshold value on an access point of an 802.11 network.
default	Configures the RxSOP threshold value on all access points of an 802.11 network.
custom_value	Custom configure the RxSOP threshold value on all access points of an 802.11 network. The range is between –85 dBm and –60 dBm.

Command Default

The default RxSOP threshold option is default.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

RxSOP determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. Higher the level, less sensitive the radio is and smaller the receiver cell size. The table below shows the RxSOP threshold values for high, medium and low levels for each 802.11 band.

Table 4: RxSOP Thresholds

802.11 Band	High Threshold	Medium Threshold	Low Threshold	Custom Threshold Value
5 GHz	–76 dBm	–78 dBm	–80 dBm	–80 dBm to –65 dBm
2.4 GHz	–79 dBm	–82 dBm	–85 dBm	–80 dBm to –65 dBm

The following example shows how to configure a high RxSOP threshold value for all access points in the 802.11a band:

```
(Cisco Controller) > config 802.11a rx-sop threshold high
```

Related Topics

config rf-profile rx-sop threshold , on page 453

config 802.11 txPower

To configure the transmit power level for all access points or a single access point in an 802.11 network, use the **config 802.11 txPower** command.

config 802.11 {**a** | **b**} **txPower** {**global** {*power_level* | **auto** | **max** | **min** | **once** } | **ap** *cisco_ap*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures the 802.11 transmit power level for all lightweight access points.
auto	(Optional) Specifies the power level is automatically set by Radio Resource Management (RRM) for the 802.11 Cisco radio.
once	(Optional) Specifies the power level is automatically set once by RRM.
power_level	(Optional) Manual Transmit power level number for the access point.
ap	Configures the 802.11 transmit power level for a specified lightweight access point.
ap_name	Access point name.

Command Default

The command default (**global**, **auto**) is for automatic configuration by RRM.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to automatically set the 802.11a radio transmit power level in all lightweight access points:

```
(Cisco Controller) > config 802.11a txPower auto
```

The following example shows how to manually set the 802.11b radio transmit power to level 5 for all lightweight access points:

```
(Cisco Controller) > config 802.11b txPower global 5
```

The following example shows how to automatically set the 802.11b radio transmit power for access point AP1:

```
(Cisco Controller) > config 802.11b txPower AP1 global
```

The following example shows how to manually set the 802.11a radio transmit power to power level 2 for access point AP1:

```
(Cisco Controller) > config 802.11b txPower AP1 2
```

Related Commands

show ap config 802.11a

config 802.11b txPower

Related Topics

config 802.11-a, on page 685

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 channel add

To add channel to the 802.11 networks auto RF channel list, use the **config advanced 802.11 channel add** command.

config advanced 802.11 {**a** | **b**} **channel add** *channel_number*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
add	Adds a channel to the 802.11 network auto RF channel list.
channel_number	Channel number to add to the 802.11 network auto RF channel list.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a channel to the 802.11a network auto RF channel list:

```
(Cisco Controller) >config advanced 802.11 channel add 132
```

Related Topics

config 802.11-a, on page 685

config advanced 802.11 channel dca anchor-time

To specify the time of day when the Dynamic Channel Assignment (DCA) algorithm is to start, use the **config advanced 802.11 channel dca anchor-time** command.

config advanced 802.11 {**a** | **b**} **channel dca anchor-time** *value*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
value	Hour of the time between 0 and 23. These values represent the hour from 12:00 a.m. to 11:00 p.m.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the time of delay when the DCA algorithm starts:

```
(Cisco Controller) > config advanced 802.11 channel dca anchor-time 17
```

Related Commands

config advanced 802.11 channel dca interval

config advanced 802.11 channel dca sensitivity

config advanced 802.11 channel

Related Topics

config advanced 802.11 channel dca chan-width-11n, on page 707

config advanced 802.11 channel dca chan-width-11n

To configure the Dynamic Channel Assignment (DCA) channel width for all 802.11n radios in the 5-GHz band, use the **config advanced 802.11 channel dca chan-width-11n** command.

config advanced 802.11 {**a** | **b**} **channel dca chan-width-11n** {**20** | **40** | **80**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
20	Sets the channel width for 802.11n radios to 20 MHz.
40	Sets the channel width for 802.11n radios to 40 MHz.
80	Sets the channel width for 802.11ac/ax radios to 80-MHz.

Command Default

The default channel width is 20.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

If you choose 40, be sure to set at least two adjacent channels in the **config advanced 802.11 channel** {**add** | **delete**} *channel_number* command (for example, a primary channel of 36 and an extension channel of 40). If you set only one channel, that channel is not used for the 40-MHz channel width.

To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20- or 40-MHz mode using the **config 802.11 chan_width** command. If you then change the static configuration to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

The following example shows how to add a channel to the 802.11a network auto channel list:

```
(Cisco Controller) >config advanced 802.11a channel dca chan-width-11n 40
```

The following example shows how to set the channel width for the 802.11ac radio as 80-MHz:

```
(Cisco Controller) >config advanced 802.11a channel dca chan-width-11n 80
```

Related Topics

config advanced 802.11 channel dca anchor-time, on page 706

config advanced 802.11 channel dca interval

To specify how often the Dynamic Channel Assignment (DCA) is allowed to run, use the **config advanced 802.11 channel dca interval** command.

config advanced 802.11 {**a** | **b**} **channel dca interval** *value*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
value	Valid values are 0, 1, 2, 3, 4, 6, 8, 12, or 24 hours. 0 is 10 minutes (600 seconds).

Command Default

The default DCA channel interval is 10 (10 minutes).

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

If your controller supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.

The following example shows how often the DCA algorithm is allowed to run:

```
(Cisco Controller) > config advanced 802.11 channel dca interval 8
```

Related Commands

config advanced 802.11 dca anchor-time

config advanced 802.11 dca sensitivity

show advanced 802.11 channel

Related Topics

config advanced 802.11 channel dca anchor-time, on page 706

config advanced 802.11 channel dca min-metric

To configure the 5-GHz minimum RSSI energy metric for DCA, use the **config advanced 802.11 channel dca min-metric** command.

config advanced 802.11 {**a** | **b**} **channel dca** *RSSI_value*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
RSSI_value	Minimum received signal strength indicator (RSSI) that is required for the DCA to trigger a channel change. The range is from –100 to –60 dBm.

Command Default

The default minimum RSSI energy metric for DCA is –95 dBm.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the minimum 5-GHz RSSI energy metric for DCA:

```
(Cisco Controller) > config advanced 802.11a channel dca min-metric -80
```

In the above example, the RRM must detect an interference energy of at least -80 dBm in RSSI for the DCA to trigger a channel change.

Related Commands

config advanced 802.11 dca interval

config advanced 802.11 dca anchor-time

show advanced 802.11 channel

Related Topics

config advanced 802.11 channel dca anchor-time, on page 706

config advanced 802.11 channel dca sensitivity

To specify how sensitive the Dynamic Channel Assignment (DCA) algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels, use the **config advanced 802.11 channel dca sensitivity** command.

config advanced 802.11 {**a** | **b**} **channel dcasensitivity** {**low** | **medium** | **high**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
low	Specifies the DCA algorithm is not particularly sensitive to environmental changes. See the "Usage Guidelines" section for more information.
medium	Specifies the DCA algorithm is moderately sensitive to environmental changes. See the "Usage Guidelines" section for more information.
high	Specifies the DCA algorithm is highly sensitive to environmental changes. See the "Usage Guidelines" section for more information.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The DCA sensitivity thresholds vary by radio band as shown in the table below.

To aid in troubleshooting, the output of this command shows an error code for any failed calls. This table explains the possible error codes for failed calls.

Table 5: DCA Sensitivity Thresholds

Sensitivity	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

The following example shows how to configure the value of DCA algorithm's sensitivity to low:

```
(Cisco Controller) > config advanced 802.11 channel dca sensitivity low
```

Related Commands

config advanced 802.11 dca interval

config advanced 802.11 dca anchor-time

show advanced 802.11 channel

Related Topics

config advanced 802.11 channel dca anchor-time, on page 706

config advanced 802.11 channel foreign

To have Radio Resource Management (RRM) consider or ignore foreign 802.11a interference avoidance in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel foreign** command.

config advanced 802.11 {**a** | **b**} **channel foreign** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the foreign access point 802.11a interference avoidance in the channel assignment.
disable	Disables the foreign access point 802.11a interference avoidance in the channel assignment.

Command Default

The default value for the foreign access point 802.11a interference avoidance in the channel assignment is enabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to have RRM consider foreign 802.11a interference when making channel selection updates for all 802.11a Cisco lightweight access points:

```
(Cisco Controller) > config advanced 802.11a channel foreign enable
```

Related Commands

show advanced 802.11a channel

config advanced 802.11b channel foreign

Related Topics

config advanced 802.11 channel load, on page 711

config advanced 802.11 channel load

To have Radio Resource Management (RRM) consider or ignore the traffic load in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel load** command.

config advanced 802.11 {**a** | **b**} **channel load** {**enable** | **disable**}

Syntax Description

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

enable	Enables the Cisco lightweight access point 802.11a load avoidance in the channel assignment.
disable	Disables the Cisco lightweight access point 802.11a load avoidance in the channel assignment.

Command Default

The default value for Cisco lightweight access point 802.11a load avoidance in the channel assignment is disabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to have RRM consider the traffic load when making channel selection updates for all 802.11a Cisco lightweight access points:

```
(Cisco Controller) > config advanced 802.11 channel load enable
```

Related Commands

show advanced 802.11a channel

config advanced 802.11b channel load

Related Topics

config advanced 802.11 channel foreign, on page 711

config advanced 802.11 channel noise

To have Radio Resource Management (RRM) consider or ignore non-802.11a noise in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel noise** command.

config advanced 802.11 {**a** | **b**} **channel noise** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables non-802.11a noise avoidance in the channel assignment. or ignore.
disable	Disables the non-802.11a noise avoidance in the channel assignment.

Command Default

The default value for non-802.11a noise avoidance in the channel assignment is disabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to have RRM consider non-802.11a noise when making channel selection updates for all 802.11a Cisco lightweight access points:

```
(Cisco Controller) > config advanced 802.11 channel noise enable
```

Related Commands

show advanced 802.11a channel

config advanced 802.11b channel noise

Related Topics

config advanced 802.11 channel foreign, on page 711

config advanced 802.11 channel outdoor-ap-dca

To enable or disable the controller to avoid checking the non-Dynamic Frequency Selection (DFS) channels, use the **config advanced 802.11 channel outdoor-ap-dca** command.

config advanced 802.11 {**a** | **b**} **channel outdoor-ap-dca** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables 802.11 network DCA list option for outdoor access point.
disable	Disables 802.11 network DCA list option for outdoor access point.

Command Default

The default value for 802.11 network DCA list option for outdoor access point is disabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The **config advanced 802.11** {**a** | **b**} **channel outdoor-ap-dca** {**enable** | **disable**} command is applicable only for deployments having outdoor access points such as 1522 and 1524.

The following example shows how to enable the 802.11a DCA list option for outdoor access point:

```
(Cisco Controller) > config advanced 802.11a channel outdoor-ap-dca enable
```

Related Commands

show advanced 802.11a channel

config advanced 802.11b channel noise

Related Topics

config advanced 802.11 channel pda-prop, on page 714

config advanced 802.11 channel pda-prop

To enable or disable propagation of persistent devices, use the **config advanced 802.11 channel pda-prop** command.

config advanced 802.11 {**a** | **b**} **channel pda-prop** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the 802.11 network DCA list option for the outdoor access point.
disable	Disables the 802.11 network DCA list option for the outdoor access point.

Command Default

The default 802.11 network DCA list option for the outdoor access point is disabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable or disable propagation of persistent devices:

```
(Cisco Controller) > config advanced 802.11 channel pda-prop enable
```

Related Topics

config advanced 802.11 channel update, on page 714

config advanced 802.11 channel update

To have Radio Resource Management (RRM) initiate a channel selection update for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel update** command.

config advanced 802.11 {**a** | **b**} **channel update**

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to initiate a channel selection update for all 802.11a network access points:

```
(Cisco Controller) > config advanced 802.11a channel update
```

Related Topics

config advanced 802.11 channel pda-prop, on page 714

config advanced 802.11 coverage

To enable or disable coverage hole detection, use the **config advanced 802.11 coverage** command.

config advanced 802.11 { **a** | **b** } **coverage** { **enable** | **disable** }

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the coverage hole detection.
disable	Disables the coverage hole detection.

Command Default

The default coverage hole detection value is enabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

If you enable coverage hole detection, the controller automatically determines, based on data that is received from the access points, whether any access points have clients that are potentially located in areas with poor coverage.

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to enable coverage hole detection on an 802.11a network:

```
(Cisco Controller) > config advanced 802.11a coverage enable
```

Related Commands

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

Related Topics

config advanced 802.11 channel update, on page 714

config advanced 802.11 coverage exception global

To specify the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point, use the **config advanced 802.11 coverage exception global** command.

config advanced 802.11 {**a** | **b**} **coverage exception global** *percent*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
percent	Percentage of clients. Valid values are from 0 to 100%.

Command Default

The default percentage value for clients on an access point is 25%.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the**config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to specify the percentage of clients for all 802.11a access points that are experiencing a low signal level:

```
(Cisco Controller) > config advanced 802.11 coverage exception global 50
```

Related Commands

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

Related Topics

config advanced 802.11 coverage fail-rate, on page 717

config advanced 802.11 coverage fail-rate

To specify the failure rate threshold for uplink data or voice packets, use the **config advanced 802.11 coverage fail-rate** command.

config advanced 802.11 {**a** | **b**} **coverage** {**data** | **voice**} **fail-rate** *percent*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
data	Specifies the threshold for data packets.
voice	Specifies the threshold for voice packets.
percent	Failure rate as a percentage. Valid values are from 1 to 100 percent.

Command Default

The default failure rate threshold uplink coverage fail-rate value is 20%.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the**config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to configure the threshold count for minimum uplink failures for data packets:

```
(Cisco Controller) > config advanced 802.11 coverage fail-rate 80
```

Related Commands

config advanced 802.11 coverage exception global

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

Related Topics

config advanced 802.11 coverage level global, on page 718
config advanced 802.11 coverage packet-count, on page 718

config advanced 802.11 coverage level global

To specify the minimum number of clients on an access point with an received signal strength indication (RSSI) value at or below the data or voice RSSI threshold, use the **config advanced 802.11 coverage level global** command.

config advanced 802.11 {**a** | **b**} **coverage level global** *clients*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
clients	Minimum number of clients. Valid values are from 1 to 75.

Command Default

The default minimum number of clients on an access point is 3.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to specify the minimum number of clients on all 802.11a access points with an RSSI value at or below the RSSI threshold:

```
(Cisco Controller) > config advanced 802.11 coverage level global 60
```

Related Commands

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

Related Topics

config advanced 802.11 coverage rssi-threshold, on page 719

config advanced 802.11 coverage packet-count

To specify the minimum failure count threshold for uplink data or voice packets, use the **config advanced 802.11 coverage packet-count** command.

config advanced 802.11 {**a** | **b**} **coverage** {**data** | **voice**} **packet-count** *packets*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
data	Specifies the threshold for data packets.
voice	Specifies the threshold for voice packets.
packets	Minimum number of packets. Valid values are from 1 to 255 packets.

Command Default

The default failure count threshold for uplink data or voice packets is10.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to configure the failure count threshold for uplink data packets:

```
(Cisco Controller) > config advanced 802.11 coverage packet-count 100
```

Related Commands

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

Related Topics

config advanced 802.11 coverage fail-rate, on page 717

config advanced 802.11 coverage rssi-threshold

To specify the minimum receive signal strength indication (RSSI) value for packets that are received by an access point, use the **config advanced 802.11 coverage rssi-threshold** command.

config advanced 802.11 {**a** | **b**} **coverage** {**data** | **voice**} **rssi-threshold** *rssi*

Syntax Description

a	Specifies the 802.11a network.

b	Specifies the 802.11b/g network.
data	Specifies the threshold for data packets.
voice	Specifies the threshold for voice packets.
rssi	Valid values are from –60 to –90 dBm.

Command Default

- The default RSSI value for data packets is –80 dBm.
- The default RSSI value for voice packets is –75 dBm.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The *rssi* value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data or voice queue with an RSSI value that is below the value that you enter, a potential coverage hole has been detected.

The access point takes RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to configure the minimum receive signal strength indication threshold value for data packets that are received by an 802.11a access point:

```
(Cisco Controller) > config advanced 802.11a coverage rssi-threshold -60
```

Related Commands

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage

Related Topics

config advanced 802.11 coverage fail-rate, on page 717

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, on page 717
config advanced 802.11 channel update, on page 714

config advanced 802.11 factory

To reset 802.11a advanced settings back to the factory defaults, use the **config advanced 802.11 factory** command.

config advanced 802.11 {**a** | **b**} **factory**

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to return all the 802.11a advanced settings to their factory defaults:

```
(Cisco Controller) > config advanced 802.11a factory
```

Related Commands

show advanced 802.11a channel

Related Topics

config advanced 802.11 group-mode, on page 724

config advanced 802.11 group-member

To configure members in 802.11 static RF group, use the **config advanced 802.11 group-member** command.

config advanced 802.11 {**a** | **b**} **group-member** {**add** | **remove**} *controller controller-ip-address*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
add	Adds a controller to the static RF group.
remove	Removes a controller from the static RF group.
controller	Name of the controller to be added.
controller-ip-address	IP address of the controller to be added.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a controller in the 802.11a automatic RF group:

```
(Cisco Controller) > config advanced 802.11a group-member add cisco-controller 209.165.200.225
```

Related Commands

show advanced 802.11a group

config advanced 802.11 group-mode

Related Topics

config advanced 802.11 group-mode, on page 724

config advanced 802.11 group-mode

To set the 802.11a automatic RF group selection mode on or off, use the **config advanced 802.11 group-mode** command.

config advanced 802.11 {**a** | **b**} **group-mode** {**auto** | **leader** | **off** | **restart**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
auto	Sets the 802.11a RF group selection to automatic update mode.
leader	Sets the 802.11a RF group selection to static mode, and sets this controller as the group leader.
off	Sets the 802.11a RF group selection to off.
restart	Restarts the 802.11a RF group selection.

Command Default

The default 802.11a automatic RF group selection mode is auto.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the 802.11a automatic RF group selection mode on:

```
(Cisco Controller) > config advanced 802.11a group-mode auto
```

The following example shows how to configure the 802.11a automatic RF group selection mode off:

```
(Cisco Controller) > config advanced 802.11a group-mode off
```

Related Commands

show advanced 802.11a group

config advanced 802.11 group-member

Related Topics

config advanced 802.11 group-member, on page 723

config advanced 802.11 logging channel

To turn the channel change logging mode on or off, use the **config advanced 802.11 logging channel** command.

config advanced 802.11 {**a** | **b**} **logging channel** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
logging channel	Logs channel changes.
on	Enables the 802.11 channel logging.
off	Disables 802.11 channel logging.

Command Default

The default channel change logging mode is Off (disabled).

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to turn the 802.11a logging channel selection mode on:

```
(Cisco Controller) > config advanced 802.11a logging channel on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging channel

Related Topics

config advanced 802.11 group-mode, on page 724

config advanced 802.11 logging coverage

To turn the coverage profile logging mode on or off, use the **config advanced 802.11 logging coverage** command.

config advanced 802.11 {**a** | **b**} **logging coverage** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 coverage profile violation logging.
off	Disables the 802.11 coverage profile violation logging.

Command Default

The default coverage profile logging mode is Off (disabled).

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to turn the 802.11a coverage profile violation logging selection mode on:

```
(Cisco Controller) > config advanced 802.11a logging coverage on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging coverage

Related Topics

config advanced 802.11 logging channel, on page 725
config advanced 802.11 logging performance, on page 728

config advanced 802.11 logging foreign

To turn the foreign interference profile logging mode on or off, use the **config advanced 802.11 logging foreign** command.

config advanced 802.11 {**a** | **b**} **logging foreign** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 foreign interference profile violation logging.
off	Disables the 802.11 foreign interference profile violation logging.

Command Default

The default foreign interference profile logging mode is Off (disabled).

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to turn the 802.11a foreign interference profile violation logging selection mode on:

```
(Cisco Controller) > config advanced 802.11a logging foreign on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging foreign

Related Topics

config advanced 802.11 logging channel, on page 725
config advanced 802.11 logging performance, on page 728

config advanced 802.11 logging load

To turn the 802.11a load profile logging mode on or off, use the **config advanced 802.11 logging load** command.

config advanced 802.11 {**a** | **b**} **logging load** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 load profile violation logging.
off	Disables the 802.11 load profile violation logging.

Command Default

The default 802.11a load profile logging mode is Off (disabled).

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to turn the 802.11a load profile logging mode on:

```
(Cisco Controller) > config advanced 802.11 logging load on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging load

Related Topics

config advanced 802.11 logging channel, on page 725
config advanced 802.11 logging performance, on page 728

config advanced 802.11 logging noise

To turn the 802.11a noise profile logging mode on or off, use the **config advanced 802.11 logging noise** command.

config advanced 802.11 {**a** | **b**} **logging noise** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 noise profile violation logging.

off	Disables the 802.11 noise profile violation logging.

Command Default

The default 802.11a noise profile logging mode is off (disabled).

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to turn the 802.11a noise profile logging mode on:

```
(Cisco Controller) > config advanced 802.11a logging noise on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging noise

Related Topics

config advanced 802.11 logging channel, on page 725
config advanced 802.11 logging performance, on page 728

config advanced 802.11 logging performance

To turn the 802.11a performance profile logging mode on or off, use the **config advanced 802.11 logging performance** command.

config advanced 802.11 {**a** | **b**} **logging performance** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 performance profile violation logging.
off	Disables the 802.11 performance profile violation logging.

Command Default

The default 802.11a performance profile logging mode is off (disabled).

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to turn the 802.11a performance profile logging mode on:

```
(Cisco Controller) > config advanced 802.11a logging performance on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging performance

Related Topics

config advanced 802.11 logging channel, on page 725
config advanced 802.11 logging load, on page 727

config advanced 802.11 logging txpower

To turn the 802.11a transmit power change logging mode on or off, use the **config advanced 802.11 logging txpower** command.

config advanced 802.11 {**a** | **b**} **logging txpower** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 transmit power change logging.
off	Disables the 802.11 transmit power change logging.

Command Default

The default 802.11a transmit power change logging mode is off (disabled).

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to turn the 802.11a transmit power change mode on:

```
(Cisco Controller) > config advanced 802.11 logging txpower off
```

Related Commands

show advanced 802.11 logging

config advanced 802.11b logging power

Related Topics

config advanced 802.11 logging channel, on page 725
config advanced 802.11 logging performance, on page 728

config advanced 802.11 monitor channel-list

To set the 802.11a noise, interference, and rogue monitoring channel list, use the **config advanced 802.11 monitor channel-list** command.

config advanced 802.11 {**a** | **b**} **monitor channel-list** {**all** | **country** | **dca**}

Syntax Description

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

all	Monitors all channels.
country	Monitors the channels used in the configured country code.
dca	Monitors the channels used by the automatic channel assignment.

Command Default

The default 802.11a noise, interference, and rogue monitoring channel list is country.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to monitor the channels used in the configured country:

```
(Cisco Controller) > config advanced 802.11 monitor channel-list country
```

Related Commands

show advanced 802.11a monitor coverage

Related Topics

config advanced 802.11 monitor signal, on page 733
config advanced 802.11 monitor load, on page 731

config advanced 802.11 monitor coverage

To set the coverage measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor coverage** command.

config advanced 802.11 {**a** | **b**} **monitor coverage** *seconds*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
seconds	Coverage measurement interval between 60 and 3600 seconds.

Command Default

The default coverage measurement interval is180 seconds.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to set the coverage measurement interval to 60 seconds:

```
(Cisco Controller) > config advanced 802.11 monitor coverage 60
```

Related Commands

show advanced 802.11a monitor

config advanced 802.11b monitor coverage

Related Topics

config advanced 802.11 monitor signal, on page 733
config advanced 802.11 monitor load, on page 731

config advanced 802.11 monitor load

To set the load measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor load** command.

config advanced 802.11 {**a** | **b**} **monitor load** *seconds*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
seconds	Load measurement interval between 60 and 3600 seconds.

Command Default

The default load measurement interval is 60 seconds.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to set the load measurement interval to 60 seconds:

```
(Cisco Controller) > config advanced 802.11 monitor load 60
```

Related Commands

show advanced 802.11a monitor

config advanced 802.11b monitor load

Related Topics

config advanced 802.11 monitor signal, on page 733
config advanced 802.11 monitor mode, on page 731

config advanced 802.11 monitor mode

To enable or disable 802.11a access point monitoring, use the **config advanced 802.11 monitor mode** command.

config advanced 802.11 {**a** | **b**} **monitor mode** {**enable** | **disable**}

Syntax Description

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

enable	Enables the 802.11 access point monitoring.
disable	Disables the 802.11 access point monitoring.

Command Default

The default 802.11a access point monitoring is enabled.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the 802.11a access point monitoring:

```
(Cisco Controller) > config advanced 802.11a monitor mode enable
```

Related Commands

show advanced 802.11a monitor

config advanced 802.11b monitor mode

Related Topics

config advanced 802.11 monitor signal, on page 733
config advanced 802.11 monitor load, on page 731

config advanced 802.11 monitor ndp-type

To configure the 802.11 access point radio resource management (RRM) Neighbor Discovery Protocol (NDP) type, use the **config advanced 802.11 monitor ndp-type** command:

config advanced 802.11 {**a** | **b**} **monitor ndp-type** {**protected** | **transparent**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
protected	Specifies the Tx RRM protected NDP.
transparent	Specifies the Tx RRM transparent NDP.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Before you configure the 802.11 access point RRM NDP type, ensure that you have disabled the network by entering the **config 802.11 disable network** command.

The following example shows how to enable the 802.11a access point RRM NDP type as protected:

```
(Cisco Controller) > config advanced 802.11 monitor ndp-type protected
```

Related Commands

config advanced 802.11 monitor

config advanced 802.11 monitor mode

config advanced 802.11 disable

Related Topics

config advanced 802.11 monitor signal, on page 733
config advanced 802.11 monitor load, on page 731

config advanced 802.11 monitor noise

To set the 802.11a noise measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor noise** command.

config advanced 802.11 {**a** | **b**} **monitor noise** *seconds*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
seconds	Noise measurement interval between 60 and 3600 seconds.

Command Default

The default 802.11a noise measurement interval is 80 seconds.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to set the noise measurement interval to 120 seconds:

```
(Cisco Controller) > config advanced 802.11 monitor noise 120
```

Related Commands

show advanced 802.11a monitor

config advanced 802.11b monitor noise

Related Topics

config advanced 802.11 monitor signal, on page 733
config advanced 802.11 monitor load, on page 731

config advanced 802.11 monitor signal

To set the signal measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor signal** command.

config advanced 802.11 {**a** | **b**} **monitor signal** *seconds*

Syntax Description

a	Specifies the 802.11a network.

b	Specifies the 802.11b/g network.
seconds	Signal measurement interval between 60 and 3600 seconds.

Command Default The default signal measurement interval is 60 seconds.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to set the signal measurement interval to 120 seconds:

```
(Cisco Controller) > config advanced 802.11 monitor signal 120
```

Related Commands

show advanced 802.11a monitor

config advanced 802.11b monitor signal

Related Topics

config advanced 802.11 monitor load, on page 731

config advanced 802.11 monitor timeout-factor

To configure the 802.11 neighbor timeout factor, use the **config advanced 802.11 monitor timeout-factor** command:

config advanced 802.11 {**a** | **b**} **monitor timeout-factor** *factor-value-in-minutes*

Syntax Description

factor-value-in-minutes	Neighbor timeout factor value that you must enter. Valid range is between 5 minutes to 60 minutes. We recommend that you set the timeout factor to 60 minutes.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

config advanced 802.11 optimized roaming

To configure the optimized roaming parameters for each 802.11 band, use the **config advanced 802.11 optimized roaming** command.

config advanced {**802.11a** | **802.11b**} **optimized-roaming** {**enable** | **disable** | **interval** *seconds* | **datarate** *mbps*}

Syntax Description

802.11a	Configures optimized roaming parameters for 802.11a network.
802.11b	Configures optimized roaming parameters for 802.11b network.
enable	Enables optimized roaming.
disable	Disables optimized roaming.
interval	Configures the client coverage reporting interval for 802.11a/b networks.
seconds	Client coverage reporting interval in seconds. The range is from 5 to 90 seconds.
datarate	Configures the threshold data rate for 802.11a/b networks.
mbps	Threshold data rate in Mbps for 802.11a/b networks. For 802.11a, the configurable data rates are 6, 9, 12, 18, 24, 36, 48, and 54. For 802.11b, the configurable data rates are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54. You can configure 0 to disable the data rate for disassociating clients.

Command Default

By default, optimized roaming is disabled. The default value for client coverage reporting interval is 90 seconds and threshold data rate is 0 (disabled state).

Command History

Release	Modification
8.8	This command was introduced.

Usage Guidelines

You must disable the 802.11a/b network before you configure the optimized roaming reporting interval. If you configure a low value for the reporting interval, the network can get overloaded with coverage report messages.

The following example shows how to enable optimized roaming for the 802.11a network:

```
(Cisco Controller) > config advanced 802.11a optimized roaming enable
```

The following example shows how to configure the data rate interval for the 802.11a network:

```
(Cisco Controller) > config advanced 802.11a optimized roaming datarate 9
```

Related Topics

show advanced 802.11 optimized roaming, on page 679

config advanced 802.11 profile foreign

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

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

Syntax Description

a	Specifies the 802.11a network.

b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access points.
cisco_ap	Cisco lightweight access point name.
percent	802.11a foreign 802.11a interference threshold between 0 and 100 percent.

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

Related Topics

config advanced 802.11 profile throughput, on page 543

config advanced 802.11 profile noise

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

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

Syntax Description

a	Specifies the 802.11a/n network.
b	Specifies the 802.11b/g/n network.
global	Configures all 802.11a Cisco lightweight access point specific profiles.
cisco_ap	Cisco lightweight access point name.
dBm	802.11a foreign noise threshold between –127 and 0 dBm.

Command Default

The default foreign noise threshold value is –70 dBm.

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

Related Topics

config advanced 802.11 profile throughput, on page 543
config advanced 802.11 profile foreign, on page 541

config advanced 802.11 profile throughput

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

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

Syntax Description

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

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

Related Topics

config advanced 802.11 profile foreign, on page 541

config advanced 802.11 profile utilization

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures a global Cisco lightweight access point specific profile.
cisco_ap	Cisco lightweight access point name.
percent	802.11a RF utilization threshold between 0 and 100 percent.

Command Default

The default RF utilization threshold value is 80 percent.

Command History

Release	Modification
8.3	This command was introduced.

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

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

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

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

Related Topics

config advanced 802.11 profile throughput, on page 543
config advanced 802.11 profile foreign, on page 541

config advanced 802.11 receiver

To set the advanced receiver configuration settings, use the **config advanced 802.11 receiver** command.

config advanced 802.11 {**a** | **b**} **receiver** {**default** | **rxstart jumpThreshold** *value*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
receiver	Specifies the receiver configuration.
default	Specifies the default advanced receiver configuration.

rxstart jumpThreshold	Specifies the receiver start signal. **Note** We recommend that you do not use this option as it is for Cisco internal use only.
value	Jump threshold configuration value between 0 and 127.

Command Default

None

Usage Guidelines

- Before you change the 802.11 receiver configuration, you must disable the 802.11 network.
- We recommend that you do not use the **rxstart jumpThreshold** *value* option as it is for Cisco internal use only.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to prevent changes to receiver parameters while the network is enabled:

```
(Cisco Controller) > config advanced 802.11 receiver default
```

Related Topics

config advanced 802.11 monitor signal, on page 733

config advanced 802.11 tpc-version

To configure the Transmit Power Control (TPC) version for a radio, use the **config advanced 802.11 tpc-version** command.

config advanced 802.11 {**a** | **b**} **tpc-version** {**1** | **2**}

Syntax Description

1	Specifies the TPC version 1 that offers strong signal coverage and stability.
2	Specifies TPC version 2 is for scenarios where voice calls are extensively used. The Tx power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there could be higher roaming delays and coverage hole incidents.

Command Default

The default TPC version for a radio is 1.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the TPC version as 1 for the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11a tpc-version 1
```

Related Commands

config advanced 802.11 tpcv1-thresh

Related Topics

config advanced 802.11 tpcv2-intense, on page 740

config advanced 802.11 tpcv1-thresh

To configure the threshold for Transmit Power Control (TPC) version 1 of a radio, use the **config advanced 802.11 tpcv1-thresh** command.

config advanced 802.11 {**a** | **b**} **tpcv1-thresh** *threshold*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g/n network.
threshold	Threshold value between –50 dBm to –80 dBm.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the threshold as –60 dBm for TPC version 1 of the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11 tpcv1-thresh -60
```

Related Commands

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv2-thresh

Related Topics

config advanced 802.11 tpc-version, on page 739

config advanced 802.11 tpcv2-intense

To configure the computational intensity for Transmit Power Control (TPC) version 2 of a radio, use the **config advanced 802.11 tpcv2-intense** command.

config advanced 802.11 {**a** | **b**} **tpcv2-intense** *intensity*

Syntax Description

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

intensity	Computational intensity value between 1 to 100.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the computational intensity as 50 for TPC version 2 of the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11 tpcv2-intense 50
```

Related Commands

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv2-thresh

config advanced 802.11 tpcv2-per-chan

Related Topics

config advanced 802.11 tpc-version, on page 739

config advanced 802.11 tpcv2-per-chan

To configure the Transmit Power Control Version 2 on a per-channel basis, use the **config advanced 802.11 tpcv2-per-chan** command.

config advanced 802.11 {**a** | **b**} **tpcv2-per-chan** {**enable** | **disable**}

Syntax Description

enable	Enables the configuration of TPC version 2 on a per-channel basis.
disable	Disables the configuration of TPC version 2 on a per-channel basis.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable TPC version 2 on a per-channel basis for the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11 tpcv2-per-chan enable
```

Related Commands

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv2-thresh

config advanced 802.11 tpcv2-intense

Related Topics

config advanced 802.11 tpc-version, on page 739

config advanced 802.11 tpcv2-thresh

To configure the threshold for Transmit Power Control (TPC) version 2 of a radio, use the **config advanced 802.11 tpcv2-thresh** command.

config advanced 802.11{**a** | **b**} **tpcv2-thresh** *threshold*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
threshold	Threshold value between –50 dBm to –80 dBm.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the threshold as –60 dBm for TPC version 2 of the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11a tpcv2-thresh -60
```

Related Commands

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv1-thresh

config advanced 802.11 tpcv2-per-chan

Related Topics

config advanced 802.11 tpc-version, on page 739

config advanced 802.11 txpower-update

To initiate updates of the 802.11a transmit power for every Cisco lightweight access point, use the **config advanced 802.11 txpower-update** command.

config advanced 802.11{**a** | **b**} **txpower-update**

Syntax Description

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

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to initiate updates of 802.11a transmit power for an 802.11a access point:

```
(Cisco Controller) > config advanced 802.11 txpower-update
```

Related Commands

config advance 802.11b txpower-update

Related Topics

config client location-calibration, on page 743

config advanced dot11-padding

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

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

Syntax Description

enable	Enables the over-the-air frame padding.
disable	Disables the over-the-air frame padding.

Command Default

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

Command History

Release	Modification
8.3	This command was introduced.

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

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

Related Commands

debug dot11

debug dot11 mgmt interface

debug dot11 mgmt msg

debug dot11 mgmt ssid

debug dot11 mgmt state-machine

debug dot11 mgmt station

show advanced dot11-padding

Related Topics

config client location-calibration, on page 743

config client location-calibration

To configure link aggregation, use the **config client location-calibration** command.

config client location-calibration {**enable** *mac_address interval* | **disable** *mac_address*}

Syntax Description

enable	(Optional) Specifies that client location calibration is enabled.

mac_address	MAC address of the client.
interval	Measurement interval in seconds.
disable	(Optional) Specifies that client location calibration is disabled.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the client location calibration for the client 37:15:85:2a with a measurement interval of 45 seconds:

```
(Cisco Controller) >config client location-calibration enable 37:15:86:2a:Bc:cf 45
```

Related Topics

debug airewave-director

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

Configuring 802.11k and Assisted Roaming

This section lists the commands for configuring, displaying, and debugging 802.11k and assisted roaming settings on the controller.

config assisted-roaming

To configure assisted roaming parameters on the controller, use the **config assisted-roaming** command.

config assisted-roaming {**denial-maximum** *count* | **floor-bias** *RSSI* | **prediction-minimum** *number_of_APs*}

Syntax Description

denial-maximum	Configures the maximum number of counts for association denial.
count	Maximum number of times that a client is denied for association when the association request that was sent to an access point does not match any access point on the prediction list. The range is from 1 to 10.
floor-bias	Configures the RSSI bias for access points on the same floor.
RSSI	RSSI bias for access points on the same floor. The range is from 5 to 25. Access points on the same floor have more preference.
prediction-minimum	Configures the minimum number of optimized access points for the assisted roaming feature.
number_of_APs	Minimum number of optimized access points for the assisted roaming feature. The range is from 1 to 6. If the number of access points in the prediction assigned to the client is smaller than this number, the assisted roaming feature does not work.

Command Default

The default RSSI bias for access points on the same floor is 15 dBm.

Usage Guidelines

802.11k allows a client to request a neighbor report that contains information about known neighbor access points, which can be used for a service set transition. The neighbor list reduces the need for active and passive scanning.

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to configure the minimum number of optimized access points for the assisted roaming feature:

```
(Cisco Controller) >config assisted-roaming prediction-minimum 4
```

Related Topics

show assisted-roaming , on page 746

config wlan assisted-roaming

To configure assisted roaming on a WLAN, use the **config wlan assisted-roaming** command.

config wlan assisted-roaming {**neighbor-list** | **dual-list** | **prediction**} {**enable** | **disable**} *wlan_id*

Syntax Description

neighbor-list	Configures an 802.11k neighbor list for a WLAN.
dual-list	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
prediction	Configures an assisted roaming optimization prediction for a WLAN.
enable	Enables the configuration on the WLAN.
disable	Disables the configuration on the WLAN.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

The 802.11k neighbor list is enabled for all WLANs.

By default, dual band list is enabled if the neighbor list feature is enabled for the WLAN.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN, if load balancing is already enabled on the WLAN.

The following example shows how to enable an 802.11k neighbor list for a WLAN:

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```

show assisted-roaming

To display assisted roaming and 802.11k configurations, use the **show assisted-roaming** command.

show assisted-roaming

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 assisted roaming and 802.11k configurations:

```
(Cisco Controller) >show assisted-roaming
Assisted Roaming and 80211k Information:
```

```
Floor RSSI Bias.................................. 15 dBm
Maximum Denial................................... 2 counts
Minimium Optimized Neighbor Assigned............. 2 neighbors

Assisted Roaming Performance Chart:
Matching Assigned Neighbor....................... [0] = 0
Matching Assigned Neighbor....................... [1] = 0
Matching Assigned Neighbor....................... [2] = 0
Matching Assigned Neighbor....................... [3] = 0
Matching Assigned Neighbor....................... [4] = 0
Matching Assigned Neighbor....................... [5] = 0
Matching Assigned Neighbor....................... [6] = 0
Matching Assigned Neighbor....................... [7] = 0
No Matching Neighbor............................. [8] = 0
No Neighbor Assigned............................. [9] = 0
```

Related Commands

config assisted-roaming

config wlan assisted-roaming

debug 11k

Related Topics

config assisted-roaming, on page 745

debug 11k

To configure the debugging of 802.11k settings, use the **debug 11k** command.

debug 11k { **all** | **detail** | **errors** | **events** | **history** | **optimization** | **simulation** } { **enable** | **disable** }

Syntax Description

all	Configures the debugging of all 802.11k messages.
detail	Configures the debugging of 802.11k details.
errors	Configures the debugging of 802.11k errors.
events	Configures the debugging of all 802.11k events.
history	Configures the debugging of all 802.11k history. The controller collects roam history of the client.
optimization	Configures the debugging of 802.11k optimizations. You can view optimization steps of neighbor lists.
simulation	Configures the debugging of 802.11k simulation data. You can view details of client roaming parameters and import them for offline simulation.
enable	Enables the 802.1k debugging.
disable	Disables the 802.1k debugging.

Command Default

None.

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to enable the debugging of 802.11k simulation data:

```
(Cisco Controller) >debug 11k simulation enable
```

Related Commands

config assisted-roaming

config wlan assisted-roaming

show assisted-roaming

Related Topics

debug dot11, on page 749
debug airewave-director

debug Commands

This section lists the **debug** commands to manage Radio Resource Management (RRM) settings of the controller.

Caution Debug commands are reserved for use only under the direction of Cisco personnel. Do not use these commands without direction from Cisco-certified staff.

debug dot11

To configure the debugging of 802.11 events, use the **debug dot11** command.

debug dot11 {**all** | **load-balancing** | **management** | **mobile** | **nmsp** | **probe** | **rldp** | **rogue** | **state**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all 802.11 messages.
load-balancing	Configures the debugging of 802.11 load balancing events.
management	Configures the debugging of 802.11 MAC management messages.
mobile	Configures the debugging of 802.11 mobile events.
nmsp	Configures the debugging of the 802.11 NMSP interface events.
probe	Configures the debugging of probe.
rldp	Configures the debugging of 802.11 Rogue Location Discovery.
rogue	Configures the debugging of 802.11 rogue events.
state	Configures the debugging of 802.11 mobile state transitions.
enable	Enables the 802.11 debugging.
disable	Disables the 802.11 debugging.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging of 802.11 settings:

```
(Cisco Controller) > debug dot11 state enable
(Cisco Controller) > debug dot11 mobile enable
```

FlexConnect Commands

show Commands

show ap flexconnect

To view the details of APs in FlexConnect mode, use the **show ap flexconnect** command.

show ap flexconnect module-vlan *ap-name*

Syntax Description

module-vlan	Displays the status of FlexConnect local switching and VLAN ID value
ap-name	Cisco AP name

Command History

Release	Modification
8.3	This command was introduced.

show capwap reap association

To display the list of clients associated with an access point and their SSIDs, use the **show capwap reap association** command.

show capwap reap association

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display clients associated to an access point and their SSIDs:

```
(Cisco Controller) >show capwap reap association
```

Related Topics

config flexconnect group

show capwap reap status, on page 752

show capwap reap status

To display the status of the FlexConnect access point (connected or standalone), use the **show capwap reap status** command.

show capwap reap status

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 command shows only the VLAN when configured as AP-specific.

The following example shows how to display the status of the FlexConnect access point:

```
(Cisco Controller) >show capwap reap status
```

Related Topics

config flexconnect group
show capwap reap association, on page 752

show flexconnect acl detailed

To display a detailed summary of FlexConnect access control lists, use the **show flexconnect acl detailed** command.

show flexconnect acl detailed *acl-name*

Syntax Description

acl-name	Name of the access control list.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the FlexConnect detailed ACLs:

```
(Cisco Controller) >show flexconnect acl detailed acl-2
```

Related Topics

config flexconnect [ipv6] acl, on page 761

show flexconnect acl summary

To display a summary of all access control lists on FlexConnect access points, use the **show flexconnect acl summary** command.

show flexconnect acl summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the FlexConnect ACL summary:

```
(Cisco Controller) >show flexconnect acl summary
ACL Name                          Status
-------------------------------- -------
acl1                             Modified
acl10                            Modified
acl1100                          Modified
acl1101                          Modified
acl1102                          Modified
acl1103                          Modified
acl1104                          Modified
acl1105                          Modified
acl1106                          Modified
```

show flexconnect group detail

To display details of a FlexConnect group, use the **show flexconnect group detail** command.

show flexconnect group detail *group_name* [**module-vlan** | **aps**]

Syntax Description

group_name	Name of the FlexConnect group.
module-vlan	Displays status of the FlexConnect local switching and VLAN ID in the group
aps	Displays list of APs that are part of the FlexConnect group

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the detailed information for a specific FlexConnect group:

```
(Cisco Controller) >show flexconnect group detail myflexgroup
Number of Ap's in Group:  1
00:0a:b8:3b:0b:c2   AP1200    Joined
Group Radius Auth Servers:
 Primary Server Index ..................... Disabled
 Secondary Server Index ................... Disabled
```

Related Topics

config flexconnect group

show flexconnect group summary

To display the current list of FlexConnect groups, use the **show flexconnect group summary** command.

show flexconnect group summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to display the current list of FlexConnect groups:

```
(Cisco Controller) >show flexconnect group summary
flexconnect Group Summary:  Count 1
Group Name         # APs
Group 1        1
```

Related Topics

config flexconnect group

config Commands

config ap flexconnect policy

To configure a policy ACL on a FlexConnect access point, use the **config ap flexconnect policy** command.

config ap flexconnect policy {**add** | **delete**} *acl_name*

Syntax Description

add	Adds a policy ACL on a FlexConnect access point.
deletes	Deletes a policy ACL on a FlexConnect access point.
acl_name	Name of the ACL.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a policy ACL on a FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect policy add acl1
```

Related Topics

config policy
config wlan policy
debug policy
show policy
show profiling policy summary

config ap flexconnect vlan

To enable or disable VLAN tagging for a FlexConnect access, use the **config ap flexconnect vlan** command.

config ap flexconnect vlan { **enable** | **disable** } *cisco_ap*

Syntax Description

enable	Enables the access point's VLAN tagging.
disable	Disables the access point's VLAN tagging.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

Disabled. Once enabled, WLANs enabled for local switching inherit the VLAN assigned at the controller.

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to enable the access point's VLAN tagging for a FlexConnect access:

```
(Cisco Controller) >config ap flexconnect vlan enable AP02
```

Related Topics

config ap flexconnect radius auth set
config ap flexconnect vlan, on page 756
config ap flexconnect vlan native, on page 757
config ap flexconnect vlan wlan, on page 758

config ap flexconnect vlan add

To add a VLAN to a FlexConnect access point, use the **config ap flexconnect vlan add** command.

config ap flexconnect vlan add *vlan-id acl in-acl out-acl cisco_ap*

Syntax Description

vlan-id	VLAN identifier.
acl	ACL name that contains up to 32 alphanumeric characters.
in-acl	Inbound ACL name that contains up to 32 alphanumeric characters.
out-acl	Outbound ACL name that contains up to 32 alphanumeric characters.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect vlan add 21 acl inacl1 outacl1 ap1
```

Related Topics

config ap flexconnect vlan, on page 756
config ap flexconnect radius auth set
config ap flexconnect vlan native, on page 757
config ap flexconnect vlan wlan, on page 758

config ap flexconnect vlan native

To configure a native VLAN for a FlexConnect access point, use the **config ap flexconnect vlan native** command.

config ap flexconnect vlan native *vlan-id cisco_ap*

Syntax Description

vlan-id	VLAN identifier.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure a native VLAN for a FlexConnect access point mode:

```
(Cisco Controller) >config ap flexconnect vlan native 6 AP02
```

Related Topics

config ap flexconnect vlan, on page 756
config ap flexconnect radius auth set
config ap flexconnect vlan add, on page 757
config ap flexconnect vlan wlan, on page 758

config ap flexconnect vlan wlan

To assign a VLAN ID to a FlexConnect access point, use the **config ap flexconnect vlan wlan** command.

config ap flexconnect vlan wlan *wlan-id vlan-id cisco_ap*

Syntax Description

wlan-id	WLAN identifier
vlan-id	VLAN identifier (1 - 4094).
cisco_ap	Name of the Cisco lightweight access point.

Command Default

VLAN ID associated to the WLAN.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to assign a VLAN ID to a FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect vlan wlan 192.12.12.1 6 AP02
```

Related Topics

config ap flexconnect vlan, on page 756
config ap flexconnect radius auth set
config ap flexconnect vlan add, on page 757

config ap flexconnect vlan native, on page 757

config ap flexconnect web-auth

To configure a FlexConnect ACL for external web authentication in locally switched WLANs, use the **config ap flexconnect web-auth** command.

config ap flexconnect web-auth wlan *wlan_id cisco_ap acl_name* { **enable** | **disable** }

Syntax Description

wlan	Specifies the wireless LAN to be configured with a FlexConnect ACL.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).
cisco_ap	Name of the FlexConnect access point.
acl_name	Name of the FlexConnect ACL.
enable	Enables the FlexConnect ACL on the locally switched wireless LAN.
disable	Disables the FlexConnect ACL on the locally switched wireless LAN.

Command Default

FlexConnect ACL for external web authentication in locally switched WLANs is disabled.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

The FlexConnect ACLs that are specific to an AP have the highest priority. The FlexConnect ACLs that are specific to WLANs have the lowest priority.

The following example shows how to enable FlexConnect ACL for external web authentication on WLAN 6:

```
(Cisco Controller) >config ap flexconnect web-auth wlan 6 AP2 flexacl2 enable
```

Related Topics

config ap flexconnect central-dhcp
config ap flexconnect local-split
config ap flexconnect radius auth set
config ap flexconnect vlan, on page 756
config ap flexconnect vlan add, on page 757
config ap flexconnect vlan native, on page 757
config ap flexconnect vlan wlan, on page 758
config ap flexconnect policy, on page 756
config ap flexconnect web-policy acl, on page 760
config ap flexconnect wlan, on page 760

config ap flexconnect web-policy acl

To configure a Web Policy FlexConnect ACL on an access point, use the **config ap flexconnect web-policy acl** command.

config ap flexconnect web-policy acl {**add** | **delete**} *acl_name*

Syntax Description

add	Adds a Web Policy FlexConnect ACL on an access point.
delete	Deletes Web Policy FlexConnect ACL on an access point.
acl_name	Name of the Web Policy FlexConnect ACL.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add a Web Policy FlexConnect ACL on an access point:

```
(Cisco Controller) >config ap flexconnect web-policy acl add flexacl2
```

Related Topics

config ap flexconnect central-dhcp
config ap flexconnect local-split
config ap flexconnect radius auth set
config ap flexconnect vlan, on page 756
config ap flexconnect vlan add, on page 757
config ap flexconnect vlan native, on page 757
config ap flexconnect vlan wlan, on page 758
config ap flexconnect policy, on page 756
config ap flexconnect web-auth, on page 759
config ap flexconnect wlan, on page 760

config ap flexconnect wlan

To configure a FlexConnect access point in a locally switched WLAN, use the **config ap flexconnect wlan** command.

config ap flexconnect wlan l2acl { **add** *wlan_id cisco_ap acl_name* | **delete** *wlan_id cisco_ap* }

Syntax Description

add	Adds a Layer 2 ACL to the FlexConnect access point.
wlan_id	Wireless LAN identifier from 1 to 512.
cisco_ap	Name of the Cisco lightweight access point.
acl_name	Layer 2 ACL name. The name can be up to 32 alphanumeric characters.

delete	Deletes a Layer 2 ACL from the FlexConnect access point.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

- You can create a maximum of 16 rules for a Layer 2 ACL.
- You can create a maximum of 64 Layer 2 ACLs on a controller.
- A maximum of 16 Layer 2 ACLs are supported per AP because an AP supports a maximum of 16 WLANs.
- Ensure that the Layer 2 ACL names do not conflict with the FlexConnect ACL names because an AP does not support the same Layer 2 and Layer 3 ACL names.

The following example shows how to configure a Layer 2 ACL on a FlexConnect AP.

```
(Cisco Controller) >config ap flexconnect wlan add 1 AP1600_1 acl_l2_1
```

Related Topics

config acl counter
config acl layer2
config wlan layer2 acl
show acl
show client detail, on page 426
show wlan, on page 436

config flexconnect [ipv6] acl

To apply access control lists that are configured on a FlexConnect access point, use the **config flexconnect** [**ipv6**] **acl** command. Use the **ipv6** keyword to configure IPv6 FlexConnect ACLs .

config flexconnect [**ipv6**] **acl** {**apply** | **create** | **delete**} *acl_name*

Syntax Description

ipv6	Use this option to configure IPv6 FlexConnect ACLs. If you don't use this option, then IPv4 FlexConnect ACLs will be configured.
apply	Applies an ACL to the data path.
create	Creates an ACL.
delete	Deletes an ACL.
acl_name	ACL name that contains up to 32 alphanumeric characters.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to apply the IPv4 ACL configured on a FlexConnect access point:

```
(Cisco Controller) >config flexconnect acl apply acl1
```

config flexconnect [ipv6] acl rule

To configure access control list (ACL) rules on a FlexConnect access point, use the **config flexconnect** [**ipv6**] **acl rule** command.

config flexconnect [**ipv6**] **acl rule** {**action** *rule_name rule_index* {**permit** | **deny**} | **add** *rule_name rule_index* | **change index** *rule_name old_index new_index* | **delete** *rule_name rule_index* | **destination address** *rule_name rule_index ip_address netmask* | **destination port range** *rule_name rule_index start_port end_port* | **direction** *rule_name rule_index* {**in** | **out** | **any**} | **dscp** *rule_name rule_index dscp* | **protocol** *rule_name rule_index protocol* | **source address** *rule_name rule_index ip_address netmask* | **source port range** *rule_name rule_index start_port end_port* | **swap index** *rule_name index_1 index_2*}

Syntax Description

ipv6	Use this option to configure IPv6 FlexConnect ACL rules. If you don't use this option, then IPv4 FlexConnect ACL rules will be configured.
action	Configures whether to permit or deny access.
rule_name	ACL name that contains up to 32 alphanumeric characters.
rule_index	Rule index between 1 and 32.
permit	Permits the rule action.
deny	Denies the rule action.
add	Adds a new rule.
change	Changes a rule's index.
index	Specifies a rule index.
delete	Deletes a rule.
destination address	Configures a rule's destination IP address and netmask.
ip_address	IP address of the rule.
netmask	Netmask of the rule.
start_port	Start port number (between 0 and 65535).
end_port	End port number (between 0 and 65535).
direction	Configures a rule's direction to in, out, or any.
in	Configures a rule's direction to in.
out	Configures a rule's direction to out.

any	Configures a rule's direction to any.
dscp	Configures a rule's DSCP.
dscp	Number between 0 and 63, or **any**.
protocol	Configures a rule's DSCP.
protocol	Number between 0 and 255, or **any**.
source address	Configures a rule's source IP address and netmask.
source port range	Configures a rule's source port range.
swap	Swaps two rules' indices.
index_1	The rule first index to swap.
index_2	The rule index to swap the first index with.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to configure an ACL to permit access:

```
(Cisco Controller) >config flexconnect acl rule action lab1 4 permit
```

config flexconnect arp-caching

To save an ARP entry for a client in the cache with locally switched WLAN on FlexConnect APs or in a software-defined access (Fabric) deployment, use **config flexconnect arp-caching** command.

config flexconnect arp-caching {**enable** } **disable**}

Syntax Description

arp-caching enable	Instructs the access point to save the ARP entry for a client in the cache and reply on its behalf of the client for locally switched WLAN.
arp-caching disable	Disables ARP caching.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

Example

The following example shows how to apply the proxy ARP with locally switched WLAN on FlexConnect APs.

```
(Cisco Controller) >config flexconnect arp-caching enable
```

config flexconnect group vlan

To configure VLAN for a FlexConnect group, use the **config flexconnect group vlan** command.

config flexconnect group *group_name* **vlan** {**add** *vlan-id* **acl** *in-aclname out-aclname* | **delete** *vlan-id*}

Syntax Description

group_name	FlexConnect group name.
add	Adds a VLAN for the FlexConnect group.
vlan-id	VLAN ID.
acl	Specifies an access control list.
in-aclname	In-bound ACL name.
out-aclname	Out-bound ACL name.
delete	Deletes a VLAN from the FlexConnect group.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add VLAN ID 1 for the FlexConnect group myflexacl where the in-bound ACL name is in-acl and the out-bound ACL is out-acl:

```
(Cisco Controller) >config flexconnect group vlan myflexacl vlan add 1 acl in-acl out-acl
```

Related Topics

debug flexconnect group, on page 772
show flexconnect group detail, on page 754
show flexconnect group summary, on page 755

config flexconnect group web-auth

To configure Web-Auth ACL for a FlexConnect group, use the **config flexconnect group web-auth** command.

config flexconnect group *group_name* **web-auth wlan** *wlan-id* **acl** *acl-name* {**enable** | **disable**}

Syntax Description

group_name	FlexConnect group name.
wlan-id	WLAN ID.

acl-name	ACL name.
enable	Enables the Web-Auth ACL for a FlexConnect group.
disable	Disables the Web-Auth ACL for a FlexConnect group.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable Web-Auth ACL webauthacl for the FlexConnect group myflexacl on WLAN ID 1:

```
(Cisco Controller) >config flexconnect group myflexacl web-auth wlan 1 acl webauthacl enable
```

Related Topics

debug flexconnect group, on page 772
show flexconnect group detail, on page 754
show flexconnect group summary, on page 755

config flexconnect group web-policy

To configure Web Policy ACL for a FlexConnect group, use the **config flexconnect group web-policy** command.

config flexconnect group *group_name* **web-policy acl** {**add** | **delete**} *acl-name*

Syntax Description

group_name	FlexConnect group name.
add	Adds the Web Policy ACL.
delete	Deletes the Web Policy ACL.
acl-name	Name of the Web Policy ACL.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to add the Web Policy ACL mywebpolicyacl to the FlexConnect group myflexacl:

```
(Cisco Controller) >config flexconnect group myflexacl web-policy acl add mywebpolicyacl
```

Related Topics

debug flexconnect group, on page 772
show flexconnect group detail, on page 754
show flexconnect group summary, on page 755

config flexconnect join min-latency

To enable or disable the access point to choose the controller with the least latency when joining, use the **config flexconnect join min-latency** command.

config flexconnect join min-latency {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the access point to choose the controller with the least latency when joining.
disable	Disables the access point to choose the controller with the least latency when joining.
cisco_ap	Cisco lightweight access point.

Command Default

The access point cannot choose the controller with the least latency when joining.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the controller that responds first.

This configuration overrides the HA setting on the controller, and is applicable only for OEAP access points.

The following example shows how to enable the access point to choose the controller with the least latency when joining:

```
(Cisco Controller) >config flexconnect join min-latency enable CISCO_AP
```

debug Commands

debug capwap reap

To configure the debugging of Control and Provisioning of Wireless Access Points (CAPWAP) settings on a FlexConnect access point, use the **debug capwap reap** command.

debug capwap reap [**mgmt** | **load**]

Syntax Description

mgmt	(Optional) Configures the debugging for client authentication and association messages.
load	(Optional) Configures the debugging for payload activities, which is useful when the FlexConnect access point boots up in standalone mode.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure the debugging of FlexConnect client authentication and association messages:

```
(Cisco Controller) >debug capwap reap mgmt
```

debug dot11 mgmt interface

To configure debugging of 802.11 management interface events, use the **debug dot11 mgmt interface** command.

debug dot11 mgmt interface

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 debug 802.11 management interface events:

```
(Cisco Controller) >debug dot11 mgmt interface
```

debug dot11 mgmt msg

To configure debugging of 802.11 management messages, use the **debug dot11 mgmt msg** command.

debug dot11 mgmt msg

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 debug dot11 management messages:

```
(Cisco Controller) >debug dot11 mgmt msg
```

debug dot11 mgmt ssid

To configure debugging of 802.11 SSID management events, use the **debug dot11 mgmt ssid** command.

debug dot11 mgmt ssid

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 debugging of 802.11 SSID management events:

```
(Cisco Controller) >debug dot11 mgmt ssid
```

debug dot11 mgmt state-machine

To configure debugging of the 802.11 state machine, use the **debug dot11 mgmt state-machine** command.

debug dot11 mgmt state-machine

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 debugging of 802.11 state machine:

```
(Cisco Controller) >debug dot11 mgmt state-machine
```

debug dot11 mgmt station

To configure the debugging of the management station settings, use the **debug dot11 mgmt station** command.

debug dot11 mgmt station

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 debugging of the management station settings:

```
(Cisco Controller) >debug dot11 mgmt station
```

debug flexconnect aaa

To configure debugging of FlexConnect backup RADIUS server events or errors, use the **debug flexconnect aaa** command.

debug flexconnect aaa {**event** | **error**} {**enable** | **disable**}

Syntax Description

event	Configures the debugging for FlexConnect RADIUS server events.
error	Configures the debugging for FlexConnect RADIUS server errors.
enable	Enables the debugging of FlexConnect RADIUS server settings.
disable	Disables the debugging of FlexConnect RADIUS server settings.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging of FlexConnect RADIUS server events:

```
(Cisco Controller) >debug flexconnect aaa event enable
```

debug flexconnect acl

Configures debugging of FlexConnect access control lists (ACLs), use the **debug flexconnect acl** command.

debug flexconnect acl {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of FlexConnect ACLs.
disable	Disables the debugging of FlexConnect ACLs.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging of FlexConnect ACLs:

```
(Cisco Controller) >debug flexconnect acl enable
```

debug flexconnect cckm

Configure debugging of FlexConnect Cisco Centralized Key Management (CCKM) fast roaming, use the **debug flexconnect cckm** command.

debug flexconnect cckm {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of FlexConnect CCKM fast roaming settings.
disable	Disables the debugging of FlexConnect CCKM fast roaming settings.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging of FlexConnect CCKM fast roaming events:

```
(Cisco Controller) >debug flexconnect cckm event enable
```

debug flexconnect client ap

To debug FlexConnect client access point MAC addresses, use the **debug flexconnect client ap** command.

debug flexconnect client ap *ap-name* {**add** | **delete**} *MAC-address1 MAC-address2 MAC-address3 MAC-address4*

Syntax Description		
	add	Adds the MAC address to the group.
	delete	Deletes the MAC address from the group.
	MAC-address	MAC address of the client

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to debug FlexConnect client ap 'room' MAC addresses:

```
(Cisco Controller) >debug flexconnect client ap room add 00.0c.41.07.33.a6 0A.0c.52.17.97.b6
```

debug flexconnect client ap syslog

To configure debug logging of the syslog server for a FlexConnect client AP, use the **debug flexconnect client ap** command.

debug flexconnect client ap *ap-name* **syslog** {*ip-address* | **disable**}

Syntax Description		
	ip-address	Configures the syslog server ip-address for debug logging.
	disable	Disables the debug logging to the syslog server.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure syslog server for debug log for the FlexConnect client AP 'room':

```
(Cisco Controller) >debug flexconnect client ap room syslog 192.168.1.1
```

debug flexconnect client group

To debug FlexConnect client group MAC addresses, use the **debug flexconnect client group** command.

debug flexconnect client group *group-name* {**add** | **delete**} *MAC-address1 MAC-address2 MAC-address3 MAC-address4*

Syntax Description		
	add	Adds the MAC address to the group.
	delete	Deletes the MAC address from the group.

MAC-address	MAC address of the client.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to debug FlexConnect client group MAC addresses:

```
(Cisco Controller) >debug flexconnect client group school add 00.0c.41.07.33.a6
0A.0c.52.17.97.b6
```

debug flexconnect client group syslog

To debug FlexConnect group access point syslog, use the **debug flexconnect client group** command.

debug flexconnect client group *group-name* **syslog** *ip-address* | *disable*

Syntax Description

ip-address	Configures the syslog server ip-address for debug logging.
disable	Disables the debug logging to the syslog server.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to configure FlexConnect client group 'school' for debug logging purposes:

```
(Cisco Controller) >debug flexconnect client group school syslog 192.168.1.1
```

debug flexconnect group

To configure debugging of FlexConnect access point groups, use the **debug flexconnect group** command.

debug flexconnect group {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of FlexConnect access point groups.
disable	Disables the debugging of FlexConnect access point groups.

Command Default None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging of FlexConnect access point groups:

```
(Cisco Controller) >debug flexconnect group enable
```

debug pem

To configure debugging of the access policy manager, use the **debug pem** command.

debug pem {**events** | **state**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of the policy manager events.
state	Configures the debugging of the policy manager state machine.
enable	Enables the debugging of the access policy manager.
disable	Disables the debugging of the access policy manager.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable the debugging of the access policy manager:

```
(Cisco Controller) >debug pem state enable
```

Mobility Express Controller Commands

Application Visibility Commands

The following commands are used to configure Application Visibility on the Cisco Mobility Express controller.

Command	Description	Added in Release
config flexconnect group default-flexgroup avc 1 visibility { enable | disable }	To enable or disable Application Visibility in a WLAN	8.1.122.0
show flexconnect group detail default-flexgroup	To display the status of Application Visibility in each WLAN	8.1.122.0
show flexconnect avc statistics group default-flexgroup	To view Application Visibility statistics based on the flex group	8.1.122.0
show flexconnect avc statistics client *client_MAC*	To view Application Visibility statistics based on each client	8.1.122.0

Cisco Umbrella Commands

The following commands are used to configure Cisco Umbrella in the Cisco Mobility Express network.

Command	Description	Added in Release
config opendns {Enable | Disable}	To configure the Cisco Umbrella feature. You can enable or disable the feature.	<8.8 MR1>
config opendns api-token	To register the Cisco Umbrella API token on the network.	<8.8 MR1>
config opendns profile {create |delete | refresh}	To create, delete, or refresh a Cisco Umbrella profile that can be applied over a WLAN	<8.8 MR1>
config wlan opendns-profile <wlan-id> <profile-name> {enable | disable}	To map the Cisco Umbrella profile identity to a WLAN.	<8.8 MR1>
config wlan opendns-dhcp-opt6 <wlan-id> {enable | disable}	To enable or disable DHCP option 6 per WLAN.	<8.8 MR1>
config wlan opendns-mode <wlan-id> {ignore | forced}	To ignore or force the Cisco Umbrella mode on the WLAN.	<8.8 MR1>
show opendns summary	To display details of Cisco Umbrella.	<8.8 MR1>

CleanAir Commands

Command	Description	Added in Release
config 802.11b cleanair enable *ap_MAC*	To enable CleanAir on an associated AP. Not applicable to 1850 and 1830 series APs.	8.1.122.0
show 802.11b cleanair device ap *ap_MAC*	To list all the interference devices connected to the AP.	8.1.122.0
show 802.11b cleanair device type jammer	To jam a specific interference device.	8.1.122.0

CMX Cloud Commands

Command	Description	Added in Release
config cloud-services server id-token *CMX_token*	To specify a valid CMX server token.	8.3.102.0
config cloud-services server url *url*	To specify a valid CMX server URL.	8.3.102.0
config cloud-services cmx enable	To enable CMX analytics.	8.3.102.0
show cloud-services cmx summary	To view details of the configured CMX cloud services.	8.3.102.0

Commands for Collecting Log, Core, and Crash Files

Command	Description	Added in Release
1. transfer upload datatype support-bundle 2. transfer upload start	Use these commands in sequence to collect log, core and crash files. The files of the following data types are collected, bundled into a .TAR file, and the uploaded to a configured TFTP or FTP server: • run-config • systemtrace • traplog • debug-file • crashfile • coredump • ap-crash-data	8.3.102.0
debug transfer all enable	To debug the code-flow, use this command before the **transfer upload start** command.	8.3.102.0
debug disable-all	To disable debugging of the code-flow.	8.3.102.0

Commands for Software Download from Cisco.com

Step	Command	Description	Added in Release
1	transfer download ap-images mode cco	To set the mode of download of software images to be from Cisco.com.	8.3.102.0
2	transfer download ap-images cco-username *username* cco-password *password*	To specify the Cisco.com credentials to be used.	8.3.102.0
3	transfer download ap-images version { suggested | latest }	To specify whether the suggested or the latest software version images are to be downloaded.	8.3.102.0
4	transfer download ap-images cco-auto-check { enable | disable }	To set the controller to automatically check for software image updates from Cisco.com.	8.3.102.0
5	transfer download start	To start the download.	8.3.102.0

Controller Image Upgrade Commands

The following commands are used when performing a Mobility Express controller software image upgrade.

Command	Description	Added in Release
transfer download ap-images imagePath *image_path*	To set the path of the software image on the TFTP server	8.1.122.0
transfer download ap-images mode tftp	To set the file transfer mode as TFTP	8.1.122.0
transfer download ap-images serverIp *ipv4_address*	To specify the IP address of the TFTP server	8.1.122.0
transfer download start	To save the configuration and start the image download	8.1.122.0
transfer download stop	To stop the ongoing image download	8.3.102.0
debug transfer all { enable | disable }	To debug the transfer and download with all sub commands enabled	8.1.122.0
debug transfer tftp { enable | disable }	To debug transfer download of TFTP	8.1.122.0
debug transfer trace { enable | disable }	To debug transfer trace	8.1.122.0

DNS Commands

Command	Description	Added in Release
config network dns default	To configure the default DNS servers.	8.2.100.1
show network summary	To view a network summary, with the default DNS servers listed, if they are enabled.	8.2.100.1

DNS ACL Commands

The following commands are used while configuring DNS IPv4 ACLs and DNS IPv6 ACLs on the Cisco Mobility Express controller.

Table 6: DNS ACL Commands

Command	Description	Command History
config flexconnect acl create *acl-name*	Creates and configures the ACL.	Introduced in 8.6.101.0
config flexconnect ipv6 acl create *acl-name*	Creates and configures the IPv6 ACL.	Introduced in 8.6.101.0
config flexconnect acl url-domain url {**snmptraps** | | **radius**} **enable** | | **disable**	Configures secure tunnel application support.	Introduced in 8.6.101.0
config secure-tunnel network{**snmptraps** | | **radius**} **enable** | | **disable**	Configures the secure tunnel network.	Introduced in 8.6.101.0
config flexconnect acl url-domain add *acl-nameindex*	Adds the URL domain to the ACL.	Introduced in 8.6.101.0
config flexconnect ipv6 acl url-domain add *acl-nameindex*	Adds the URL domain to the IPv6 ACL.	
config flexconnect acl url-domain url *acl-nameindexurl-name*	Configures the URL name in the ACL.	Introduced in 8.6.101.0
config flexconnect ipv6 acl url-domain url *acl-nameindexurl-name*	Configures the URL name in the IPv6 ACL.	
config flexconnect acl url-domain delete *acl-nameindex*	Deletes the URL domain from the ACL.	Introduced in 8.6.101.0
config flexconnect ipv6 acl url-domain delete *acl-nameindex*	Deletes the IPv6 URL domain from the ACL.	
config flexconnect acl url-domain action *acl-nameindex permit* | *deny*	Configures the action of an ACL rule.	Introduced in 8.6.101.0
config flexconnect ipv6 acl url-domain action *acl-nameindex permit* | *deny*	Configures the action of an IPv6 ACL rule.	

Command	Description	Command History
config flexconnect group *group-name***policy acl {add | delete}***acl-name*	Adds or deletes policy IPv4 ACL on the Flexconnect group.	Introduced in 8.6.101.0
config flexconnect group *group-name***policy ipv6 acl {add | delete}***acl-name*	Adds or deletes policy IPv6 ACL on the Flexconnect group.	
config flexconnect acl apply *acl-name*	Applies the IPv4 ACL to the APs.	
config flexconnect ipv6 acl apply *acl-name*	Applies the IPv6 ACL to the APs.	
config flexconnect group *group-name***web-auth wlan***wlan-id***acl***acl-name***{enable | disable}**	Configures WLAN for web-auth IPv4 ACL on the Flexconnect group.	Introduced in 8.6.101.0
config flexconnect group *group-name***web-auth wlan***wlan-id* **ipv6 acl***acl-name***{enable | disable}**	Configures WLAN for web-auth IPv6 ACL on the Flexconnect group.	Introduced in 8.6.101.0
show flexconnect acl {summary | detailed *acl-name***}**	Displays the summary of the Access Control Lists or the detailed Access Control List information.	Introduced in 8.6.101.0
show flexconnect ipv6acl {summary | detailed *acl-name***}**	Displays the summary of the IPv6 Access Control Lists or the detailed IPv6 Access Control List information.	Introduced in 8.6.101.0

Efficient AP Join Command

The following command is used to configure the efficient AP join in the Cisco Mobility Express network.

Command	Description	Added in Release
config flexconnect group default-flexgroup efficient-join {enable | disable}	To configure efficient join.	8.8.100.0

EoGRE Commands

The following commands are available once Ethernet over GRE (EoGRE) configurations are enabled for the Cisco Mobility Express network. EoGRE tunnels in Cisco Mobility Express only support FlexConnect mode.

Command	Description	Added in Release
config tunnel	To add or delete custom CCX multicast addresses for RFID tag tracking. The addresses that can be configured include **0x01**, **0x40**, **0x96**, **0x00**, and **0x03**.	8.8.100.0
config tunnel	To	8.8.100.0
config tunnel	To	8.8.100.0
config tunnel	To	8.8.100.0
config tunnel profile rule add *profile-name* **realm-filter** *realm-string* **eogre vlan***vlan-id domain-name*	To add a new rule to the profile.	8.8.100.0
config tunnel profile rule delete *profile-name* **realm-filter** *realm-string*	To delete an existing rule from the profile.	8.8.100.0
config tunnel profile rule modify *profile-name* **realm-filter** *realm-string* **eogre vlan***vlan-id domain-name*	To modify an existing rule.	8.8.100.0
config tunnel	To	8.8.100.0
config tunnel	To	8.8.100.0
config tunnel	To	8.8.100.0
config tunnel	To	8.8.100.0
config tunnel	To	8.8.100.0
config tunnel	To	8.8.100.0
config rfid rate-limit	To configure the RFID message rate limit over a cycle of processing.	8.8.100.0

Command	Description	Added in Release
config rfid status {enable | disable}	To enable or disable RFID tag data collection.	8.8.100.0
config rfid timeout	To configure the RFID tag data timeout.	8.8.100.0
show rfid client	To display the summary of RFID tags that are clients.	8.8.100.0
show rfid config	To display the configuration options for RFID tag tracking.	8.8.100.0
show rfid detail	To display detailed information for a specified RFID tag.	8.8.100.0
show rfid summary	To display summary information for all known RFID tags.	8.8.100.0

Migration Commands

The following commands are used for converting an AP from Mobility Express software image to Lightweight CAPWAP AP software image, and vice-versa.

Command	Description	Added in Release
ap-type capwap	To convert ap-type from Mobility Express to CAPWAP	8.1.122.0
ap-type mobilityexpress tftp://*tftp_server*/*file_name*	To convert ap-type from CAPWAP to Mobility Express, when running an Mobility Express software image	8.1.122.0
config ap unifiedmode *switch_name switch_IP_address*	To convert all APs to type CAPWAP simultaneously from the switch	8.1.122.0

mDNS Commands

The following commands are used to configure multicast DNS in the Cisco Mobility Express network.

Command	Description	Added in Release
config mdns policy {disable | **enable** | **service-group}**	To configure the mDNS policy. You can enable or disable and mDNS access policy, and also configure and mDNS service group.	Introduced in 8.8.120.0
config mdns policy service-group create <*service-group-name*> [<*service-group-description*>]	To create an mDNS service group, enter the service group name and the description.	Introduced in 8.8.120.0
config mdns policy service-group delete <*service-group-name*>	To delete an mDNS service group, enter the service group name.	Introduced in 8.8.120.0
config mdns policy service-group device-mac {add <*service-group-name*> <*mac-addr*> <*device-name*> <*location-type*> <*device-location*> | **delete** <*service-group-name*> <*mac-addr*>}	To add a device-mac to the mDNS service group, enter the service group name, MAC address, the device name, and the location type. Enter the device location type as AP_LOCATION, or AP_NAME, or AP_GROUP. To delete a device-mac, enter the service group name and the MAC address.	Introduced in 8.8.120.0
config mdns policy service-group user-name {add | **delete}** <*service-group-name*> <*user-name*>	To add or delete the mDNS policy service group username, enter the service group name and the username.	Introduced in 8.8.120.0
config mdns policy service-group user-role {add | **delete}** <*service-group-name*> <*user-name*>	To add or delete the mDNS policy service group user role, enter the service group name and the username.	Introduced in 8.8.120.0

Command	Description	Added in Release
show mdns policy service-group {summary | detailed *<service-group-name>*}	To view the mDNS access policy status, total number of mDNS policies, and number of admin configured policies. The **summary** keyword displays the access policy status, total number of mDNS policies, and number of admin configured policies. The **detailed**keyword displays details of a particular service group name.	Introduced in 8.8.120.0
clear mdns service-database	To clear the mDNS service database.	8.8.100.0
config mdns service	To configure the mDNS service. You can create a service, mention the origin, enable or disable a query, and delete a service.	8.8.100.0
config mdns service lss	To enable or disable location specific service on a specific mDNS service or all mDNS services.	8.8.100.0
config mdns service origin	To configure learning of services from wired, wireless, or both.	8.8.100.0
config mdns snooping {enable | disable}	To enable mDNS snooping on the WLAN.	8.8.100.0
config mdns profile {create | delete}	To configure an mDNS profile.	8.8.100.0
config wlan mdns {enable | disable}	To configure mDNS for a WLAN.	8.8.100.0
config wlan mdns profile	To map an mDNS profile to a WLAN.	8.8.100.0
config mdns query interval	To set the value of the mDNS query in minutes.	8.8.100.0

Command	Description	Added in Release
config mdns service	To configure the mDNS service. You can create a service, mention the origin, enable or disable a query, and delete a service.	8.8.100.0
config mdns service query {enable | disable}	To configure a query for an mDNS service.	8.8.100.0
config mdns profile service {add | delete}	To configure an mDNS profile to a service	8.8.100.0
show client detail	To view the mDNS profile for a client.	8.8.100.0
show mdns domain-name-ip summary	To view information about the mDNS domain names.	8.8.100.0
show mdns profile	To display the information about all mDNS profiles or a particular mDNS profile.	8.8.100.0
show mdns service	To display the information about all mDNS services or a particular mDNS service.	8.8.100.0
show network summary	To view the mDNS details for a network.	8.8.100.0
show wlan	To view information about an mDNS profile that is associated with a WLAN.	8.8.100.0

Next Preferred Primary AP and Forced Failover

Command	Description	Added in Release
config ap next-preferred-master *cisco_ap_name*	To set the next preferred primary AP.	8.3.102.0
config ap next-preferred-master *cisco_ap_name* forced-failover	To set the next preferred primary AP and to manually trigger a failover to that AP.	8.3.102.0

NTP Commands

Command	Description	Added in Release
config time ntp server 1 *FQDN_of_server*	To configure the fully qualified domain name of the NTP server having, for example here, NTP index 1.	8.2.100.1
config time ntp server 2 *NTP_Server_IP_address*	To configure the IP address of the NTP server having, for example here, NTP index 2.	8.2.100.1

RFID Commands

The following commands are used to configure and monitor tracking of Radio Frequency Identifier (RFID) tags in the Cisco Mobility Express network.

Command	Description	Added in Release
config rfid ccx	To add or delete custom CCX multicast addresses for RFID tag tracking. The addresses that can be configured include **0x01**, **0x40**, **0x96**, **0x00**, and **0x03**.	8.8.100.0
config rfid rate-limit	To configure the RFID message rate limit over a cycle of processing.	8.8.100.0
config rfid status {enable | disable}	To enable or disable RFID tag data collection.	8.8.100.0
config rfid timeout	To configure the RFID tag data timeout.	8.8.100.0
show rfid client	To display the summary of RFID tags that are clients.	8.8.100.0
show rfid config	To display the configuration options for RFID tag tracking.	8.8.100.0
show rfid detail	To display detailed information for a specified RFID tag.	8.8.100.0
show rfid summary	To display summary information for all known RFID tags.	8.8.100.0

TLS Gateway Commands

The following commands are used while configuring a secure TLS tunnel to enable the Cisco Mobility Express controller to communicate with the TLS gateway.

Note TLS Gateway does not support Cisco Mobility Express platform.

Table 7: TLS Secure Tunnel Gateway Commands

Command	Description	Command History
config secure-tunnel gateway{**fqdn** | | **ip-address** | | **ip-address**}	Configures the TLS secure tunnel gateway parameters: gateway FQDN, gateway IP Address, and gateway port.	Introduced in 8.6.101.0
config secure-tunnel psk{**identity** | | **key**}	Configures secure tunnel PSK cipher parameters.	Introduced in 8.6.101.0
config secure-tunnel application{**snmptraps** | | **radius**} **enable** | | **disable**	Configures secure tunnel application support.	Introduced in 8.6.101.0
config secure-tunnel network{**snmptraps** | | **radius**} **enable** | | **disable**	Configures the secure tunnel network.	Introduced in 8.6.101.0
config secure-tunnel enable | | **disable**	Configures secure tunnel support.	Introduced in 8.6.101.0
show secure-tunnel summary	Displays the summary of the secure tunnel configuration and the secure tunnel runtime information.	Introduced in 8.6.101.0
show secure-tunnel detail	Displays the details of the secure tunnel configured networks, runtime information, Cloud DNS servers, secure tunnel routes and so on.	Introduced in 8.6.101.0
show secure-tunnel statistics	Displays the secure tunnel statistics.	Introduced in 8.6.101.0
show secure-tunnel debug-info	Displays the debug information of the secure tunnel.	Introduced in 8.6.101.0

VRRP Commands

The following Virtual Router Redundancy Protocol (VRRP) commands are used during the Mobility Express controller failover and for the primary AP.

Command	Description	Added in Release
config ap next-preferred-master	To configure the primary AP that has been elected to take over as the new primary AP	8.1.122.0
show ap next-preferred-master	To display the status of the primary AP	8.1.122.0
clear ap next-preferred-master	To clear the configuration of the primary AP	8.1.122.0
show mob-exp vrrp vrid	To display the VRID.	8.8.100.0
show mob-exp vrrp mac	To display the VRRP MAC	8.8.100.0
config mob-exp vrid *new_vrid*	To configure a new VRID. The range for *new_vrid* is 1 to 255 where the default is 1.	8.8.100.0

WLAN Security Commands

Command	Description	Added in Release
config wlan security wpa akm cckm {enable | disable} wlan_id	To enable or disable CCKM	8.2.100.1