



Cisco Wireless LAN Controller System Management Command Reference, Release 7.4

First Published: December 17, 2012

Last Modified: January 28, 2013

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

Text Part Number: OL-28146-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface xix

Audience xix

Document Organization xix

Document Conventions xix

Related Documentation xxii

Obtaining Documentation and Submitting a Service Request xxii

CHAPTER 1

Overview 1

CLI Command Keyboard Shortcuts 1

Using the Interactive Help Feature 2

Using the Help Command 3

Using the ? command 4

Using the partial? command 4

Using the partial command<tab> 5

Using the command ? 5

command keyword ? 6

CHAPTER 2

CLI Commands 7

Show Commands 7

Show AVC Commands 8

show avc applications 9

show avc profile 11

show avc statistics application 12

show avc statistics client 14

show avc statistics guest-lan 16

show avc statistics remote-lan 18

show avc statistics top-apps 20

show avc statistics wlan	22
Show CAC Commands	23
show cac voice stats	24
show cac voice summary	26
show cac video stats	27
show cac video summary	28
Show Client Commands	29
show client calls	30
show client roam-history	31
show client summary	32
show client summary guest-lan	33
show client tsm	34
show client username	35
show client voice-diag	36
show flow exporter	37
show flow monitor summary	38
Show mDNS Commands	38
show mdns profile	39
show mnds service	41
Show Radio Frequency ID Commands	43
show rfid client	44
show rfid config	45
show rfid detail	46
show rfid summary	47
Other Show Commands	47
show 802.11 cu-metrics	48
show advanced 802.11 l2roam	49
show advanced send-disassoc-on-handoff	50
show advanced sip-preferred-call-no	51
show advanced sip-snooping-ports	52
show arp kernel	53
show arp switch	54
show boot	55
show band-select	56
show buffers	57

show cdp	58
show certificate lsc	59
show certificate ssc	60
show certificate summary	61
show coredump summary	62
show cpu	63
show custom-web	64
show database summary	65
show dhcp	66
show dtls connections	68
show dhcp proxy	69
show dhcp timeout	70
show guest-lan	71
show invalid-config	72
show inventory	73
show license agent	74
show license all	75
show license capacity	77
show license detail	78
show license expiring	79
show license evaluation	80
show license feature	81
show license file	82
show license handle	83
show license image-level	84
show license in-use	85
show license permanent	86
show license status	87
show license statistics	88
show license summary	89
show license udi	90
show load-balancing	91
show logging	92
show loginsession	94
show mgmtuser	95

show netuser	96
show netuser guest-roles	97
show network	98
show network summary	99
show network multicast mgid detail	101
show network multicast mgid summary	102
show nmsp notify-interval summary	103
show nmsp statistics	104
show nmsp status	106
show nmsp subscription	107
show ntp-keys	108
show qos	109
show reset	110
show route kernel	111
show route summary	112
show sessions	113
show snmpcommunity	114
show snmpengineID	115
show snmptrap	116
show snmpv3user	117
show snmpversion	118
show switchconfig	119
show sysinfo	120
show tech-support	121
show time	122
show trapflags	124
show traplog	126
Config Commands	126
Configure 802.11h Commands	127
config 802.11h channelswitch	128
config 802.11h powerconstraint	129
config 802.11h setchannel	130
Configure 802.11 11n Support Commands	131
config 802.11 11n support	132
config 802.11 11n support a-mpdu tx priority	133

config 802.11 11n support a-mpdu tx scheduler	135
config 802.11 11n support antenna	136
config 802.11 11n support guard-interval	137
config 802.11 11n support mcs tx	138
config 802.11 11n support rifs	140
Configure 802.11 CAC Commands	141
config 802.11 cac defaults	142
config 802.11 cac video acm	144
config 802.11 cac video cac-method	145
config 802.11 cac video load-based	147
config 802.11 cac video max-bandwidth	149
config 802.11 cac media-stream	151
config 802.11 cac multimedia	153
config 802.11 cac video roam-bandwidth	155
config 802.11 cac video sip	157
config 802.11 cac video tspec-inactivity-timeout	159
config 802.11 cac voice acm	161
config 802.11 cac voice max-bandwidth	162
config 802.11 cac voice roam-bandwidth	164
config 802.11 cac voice tspec-inactivity-timeout	166
config 802.11 cac voice load-based	168
config 802.11 cac voice max-calls	170
config 802.11 cac voice sip bandwidth	172
config 802.11 cac voice sip codec	174
config 802.11 cac voice stream-size	176
Config 802.11 Commands	177
config 802.11 beacon period	178
config 802.11 disable	179
config 802.11 dtpe	180
config 802.11 enable	181
config 802.11 exp-bwreq	182
config 802.11 fragmentation	183
config 802.11 l2roam rf-params	184
config 802.11 max-clients	186
config 802.11 multicast data-rate	187

config 802.11 rate	188
config 802.11 tsm	189
Configure Advanced 802.11 Commands	190
config advanced 802.11 7920VSIEConfig	191
config advanced 802.11 edca-parameters	192
config advanced fastpath fastcache	193
config advanced fastpath pkt-capture	194
config advanced sip-preferred-call-no	195
config advanced sip-snooping-ports	196
Configure AVC Commands	196
config avc profile create	197
config avc profile delete	198
config avc profile rule	199
config wlan avc	201
Configure Band-Select Commands	203
config band-select cycle-count	204
config band-select cycle-threshold	205
config band-select expire	206
config band-select client-rssi	207
Configure Guest-LAN Commands	208
config guest-lan	209
config guest-lan custom-web ext-webauth-url	210
config guest-lan custom-web global disable	211
config guest-lan custom-web login_page	212
config guest-lan custom-web webauth-type	213
config guest-lan ingress-interface	214
config guest-lan interface	215
config guest-lan mobility anchor	216
config guest-lan nac	217
config guest-lan security	218
Configure mDNS Commands	218
config interface group mdns-profile	219
config interface mdns-profile	220
config mdns profile	221
config mdns query interval	223

config mdns service	224
config mdns snooping	226
config wlan mdns	227
Configure Management-User Commands	229
config mgmtuser add	230
config mgmtuser delete	231
config mgmtuser description	232
config mgmtuser password	233
Configure Net User Commands	234
config netuser add	235
config netuser delete	237
config netuser description	238
config netuser guest-lan-id	239
config netuser guest-role apply	240
config netuser guest-role create	241
config netuser guest-role delete	242
config netuser guest-role qos data-rate average-data-rate	243
config netuser guest-role qos data-rate average-realtime-rate	244
config netuser guest-role qos data-rate burst-data-rate	245
config netuser guest-role qos data-rate burst-realtime-rate	246
config netuser lifetime	247
config netuser maxUserLogin	248
config netuser password	249
config netuser wlan-id	250
Configure Network Commands	251
config network 802.3-bridging	252
config network allow-old-bridge-aps	253
config network ap-discovery	254
config network ap-fallback	255
config network ap-priority	256
config network apple-talk	257
config network arptimeout	258
config network bridging-shared-secret	259
config network broadcast	260
config network fast-ssid-change	261

config network ip-mac-binding	262
config network master-base	263
config network mgmt-via-wireless	264
config network multicast global	265
config network multicast igmp query interval	266
config network multicast igmp snooping	267
config network multicast igmp timeout	268
config network multicast l2mcast	269
config network multicast mld	270
config network multicast mode multicast	271
config network multicast mode unicast	272
config network oeap-600 dual-rlan-ports	273
config network oeap-600 local-network	274
config network otap-mode	275
config network rf-network-name	276
config network secureweb	277
config network secureweb cipher-option	278
config network ssh	279
config network telnet	280
config network usertimeout	281
config network web-auth captive-bypass	282
config network web-auth cmcc-support	283
config network web-auth port	284
config network web-auth proxy-redirect	285
config network web-auth secureweb	286
config network webmode	287
config network web-auth	288
config network zero-config	289
Configure QoS Commands	289
config qos average-data-rate	290
config qos average-realtime-rate	291
config qos burst-data-rate	292
config qos burst-realtime-rate	293
config qos description	294
config qos max-rf-usage	295

config qos dot1p-tag	296
config qos priority	297
config qos protocol-type	299
config qos queue_length	300
Configure SNMP Commands	301
config snmp community accessmode	302
config snmp community create	303
config snmp community delete	304
config snmp community ipaddr	305
config snmp community mode	306
config snmp engineID	307
config snmp syscontact	308
config snmp syslocation	309
config snmp trapreceiver create	310
config snmp trapreceiver delete	311
config snmp trapreceiver mode	312
config snmp v3user create	313
config snmp v3user delete	315
config snmp version	316
Configure Trap Flag Commands	317
config trapflags 802.11-Security	318
config trapflags aaa	319
config trapflags adjchannel-rogueap	320
config trapflags ap	321
config trapflags authentication	322
config trapflags client	323
config trapflags client max-warning-threshold	324
config trapflags configsave	325
config trapflags IPsec	326
config trapflags linkmode	327
config trapflags mesh	328
config trapflags multiusers	329
config trapflags rfid	330
config trapflags rogueap	332
config trapflags rrm-params	333

config trapflags rrm-profile	334
config trapflags stpmode	335
config trapflags strong-pwdcheck	336
config trapflags wps	337
Other Config Commands	337
config boot	338
config cdp	339
config certificate	340
config certificate lsc	341
config certificate ssc	343
config certificate use-device-certificate webadmin	344
config coredump	345
config coredump ftp	346
config coredump username	347
config custom-web ext-webauth-mode	348
config custom-web ext-webauth-url	349
config custom-web ext-webserver	350
config custom-web logout-popup	351
config custom-web redirectUrl	352
config custom-web webauth-type	353
config custom-web weblogo	354
config custom-web webmessage	355
config custom-web webtitle	356
config dhcp	357
config dhcp proxy	360
config dhcp timeout	361
config flow	362
config license agent	363
config license boot	365
config load-balancing	366
config location	368
config logging buffered	370
config logging console	371
config logging debug	372
config logging fileinfo	373

config logging procinfo	374
config logging traceinfo	375
config logging syslog host	376
config logging syslog facility	377
config logging syslog level	379
config login session close	380
config nmsp notify-interval measurement	381
config paging	382
config passwd-clear text	383
config prompt	384
config rfid auto-timeout	385
config rfid status	386
config rfid timeout	387
config service timestamps	388
config sessions maxsessions	389
config sessions timeout	390
config switchconfig boot-break	391
config switchconfig fips-prerequisite	392
config switchconfig strong-pwd	393
config switchconfig flowcontrol	394
config switchconfig mode	395
config switchconfig secret-obfuscation	396
config sysname	397
config time manual	398
config time ntp	399
config time timezone	401
config time timezone location	402
config wlan flow	405
Saving Configurations	405
save config	406
Timeout Commands	406
config 802.11 cac video tspec-inactivity-timeout	407
config 802.11 cac voice tspec-inactivity-timeout	409
config advanced timers ap-discovery-timeout	411
config advanced timers ap-heartbeat-timeout	412

config advanced timers ap-primary-discovery-timeout	413
config advanced timers auth-timeout	414
config advanced timers eap-timeout	415
config dhcp timeout	416
config ldap	417
config remote-lan session-timeout	418
config network usertimeout	419
config radius acct retransmit-timeout	420
config radius auth mgmt-retransmit-timeout	421
config radius auth retransmit-timeout	422
config radius auth server-timeout	423
config rogue ap timeout	424
config tacacs athr mgmt-server-timeout	425
config tacacs auth mgmt-server-timeout	426
config rfid auto-timeout	427
config rfid timeout	428
config wlan session-timeout	429
config wlan usertimeout	430
config wlan security wpa akm ft	431
config wlan security ft	432
Clearing Configurations, Log files, and Other Actions	432
clear acl counters	433
clear ap-config	434
clear ap-eventlog	435
clear ap join stats	436
clear arp	437
clear avc statistics	438
clear client tsm	440
clear config	441
clear ext-webauth-url	442
clear license agent	443
clear location rfid	444
clear location statistics rfid	445
clear loop statistics	446
clear login-banner	447

clear lwapp private-config	448
clear mdns service-database	449
clear nmsp statistics	450
clear radius acct statistics	451
clear tacacs auth statistics	452
clear redirect-url	453
clear stats ap wlan	454
clear stats local-auth	455
clear stats mobility	456
clear stats port	457
clear stats radius	458
clear stats switch	459
clear stats tacacs	460
clear transfer	461
clear traplog	462
clear webimage	463
clear webmessage	464
clear webtitle	465
Resetting the System Reboot Time	465
reset system at	466
reset system in	467
reset system cancel	468
reset system notify-time	469
reset peer-system	470
Uploading and Downloading Files and Configurations	470
transfer download certpasswor	471
transfer download datatype	472
transfer download filename	473
transfer download mode	474
transfer download password	475
transfer download path	476
transfer download port	477
transfer download serverip	478
transfer download start	480
transfer download tftpPktTimeout	481

transfer download tftpMaxRetries	482
transfer download username	483
transfer encrypt	484
transfer upload datatype	485
transfer upload filename	487
transfer upload mode	488
transfer upload pac	489
transfer upload password	490
transfer upload path	491
transfer upload peer-start	492
transfer upload port	493
transfer upload serverip	494
transfer upload start	495
transfer upload username	496
Installing and Modifying Licenses on Cisco 5500 Series Controllers	496
license clear	498
license comment	499
license install	500
license modify priority	501
license revoke	503
license save	504
Configure Right to Use (RTU) Licensing Commands	504
license activate ap-count eval	505
license activate feature	506
license add ap-count	507
license add feature	508
license deactivate ap-count eval	509
license deactivate feature	510
license delete ap-count	511
license delete feature	512
Troubleshooting the Controller Settings	512
debug arp	513
debug avc error	514
debug avc events	515
debug cac	516

debug crypto	517
debug dhcp	518
debug dhcp service-port	519
debug disable-all	520
debug l2age	521
debug mac	522
debug mdns all	523
debug mdns detail	524
debug mdns error	525
debug mdns message	526
debug memory	527
debug nmsp	528
debug ntp	529
debug poe	530
debug rbcg	531
debug rfid	532
debug snmp	533
debug transfer	534
debug voice-diag	535
show debug	536
show eventlog	537
show memory monitor	538
show run-config	539
show process	540
show tech-support	541
Configure Memory Monitor Commands	542
config memory monitor errors	543
config memory monitor leaks	544
Configure Message Log Level Commands	546
config msglog level critical	547
config msglog level error	548
config msglog level security	549
config msglog level verbose	550
config msglog level warning	551



Preface

This preface describes the audience, organization, and conventions of the Cisco Wireless LAN Controller Command Reference Guide. It also provides information on how to obtain other documentation. This chapter includes the following sections:

- [Audience, page xix](#)
- [Document Organization, page xix](#)
- [Document Conventions, page xix](#)
- [Related Documentation, page xxii](#)
- [Obtaining Documentation and Submitting a Service Request, page xxii](#)

Audience

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

Document Organization

This document is organized into the following chapters:

Chapter	Description
Overview	Describes how to use the command-line interface (CLI) on the controller.
CLI Commands	Provides detailed information about the CLI commands for the controller.

Document Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font.
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic</i> font.
[]	Elements in square brackets are optional.
{ x y z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[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.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier</code> 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).)
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 físicos. 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").

Warning Title	Description
¡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 Unified Wireless Network solution:

- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller System Message Guide*
- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*

Obtaining Documentation and Submitting a Service Request

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.



Overview

- [CLI Command Keyboard Shortcuts](#), page 1
- [Using the Interactive Help Feature](#), page 2
- [Using the Help Command](#), page 3
- [Using the ? command](#), page 4
- [Using the partial? command](#), page 4
- [Using the partial command<tab>](#), page 5
- [Using the command ?](#), page 5
- [command keyword ?](#), page 6

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 l
	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

Action	Description	Keyboard Shortcut
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 an 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
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 following table lists the interactive help feature list.

Table 2: Interactive Help Feature List

Command	
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?).

Examples

```
> 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.

Examples

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 complete a partial command name, use the partial command<tab> command.

partial command<tab>

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

Examples

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

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

Using the command ?

Examples

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

command ?

There should be 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 ?

Usage Guidelines

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

Examples

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



CLI Commands

The Cisco Wireless LAN solution command-line interface (CLI) enables operators to connect an ASCII console to the Cisco Wireless LAN Controller and configure the controller and its associated access points.

- [Show Commands, page 7](#)
- [Other Show Commands, page 47](#)
- [Config Commands, page 126](#)
- [Resetting the System Reboot Time, page 465](#)
- [Uploading and Downloading Files and Configurations, page 470](#)
- [Installing and Modifying Licenses on Cisco 5500 Series Controllers, page 496](#)
- [Configure Right to Use \(RTU\) Licensing Commands, page 504](#)
- [Troubleshooting the Controller Settings, page 512](#)

Show Commands

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

Show AVC Commands

Use **show avc** commands to display Application Visibility and Control (AVC) settings.

show avc applications

To display all the supported Application Visibility and Control (AVC) applications, use the **show avc applications** command.

show avc applications

Syntax Description This command has no arguments or keywords.

Command Default None.

Usage Guidelines AVC uses the Network-Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1500 Layer 4 to Layer 7 protocols.

Examples This example shows how to display all the supported AVC applications:

> **show avc applications**

Application-Name =====	App-ID =====	Engine-ID =====	Selector-ID =====	Application-Group-Name =====
3com-amp3	538	3	629	other
3com-tsmux	977	3	106	obsolete
3pc	788	1	34	layer3-over-ip
914c/g	1109	3	211	net-admin
9pfs	479	3	564	net-admin
acap	582	3	674	net-admin
acas	939	3	62	other
accessbuilder	662	3	888	other
accessnetwork	607	3	699	other
acp	513	3	599	other
acr-nema	975	3	104	industrial-protocols
active-directory	1194	13	473	other
activesync	1419	13	490	business-and-productivity-tools
adobe-connect	1441	13	505	other
aed-512	963	3	149	obsolete
afpovertcp	1327	3	548	business-and-productivity-tools
agentx	609	3	705	net-admin
alpes	377	3	463	net-admin
aminet	558	3	2639	file-sharing
an	861	1	107	layer3-over-ip
----	----	----	----	-----

Related Commands

- config avc profile delete
- config avc profile create
- config avc profile rule
- config wlan avc
- show avc profile
- show avc applications

show avc statistics

debug avc error

debug avc events

show avc profile

To display Application Visibility and Control (AVC) profiles, use the **show avc profile** command.

show avc profile {**summary** | **detailed** *profile_name* }

Syntax Description

summary	Displays a summary of AVC profiles.
detailed	Displays the details of an AVC profile.
<i>profile_name</i>	Name of the AVC profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

None.

Examples

This example shows how to display a summary of AVC profiles:

```
> show avc profile summary
Profile-Name                      Number of Rules
=====
profile 1                          3
avc_profile2                       1
```

This example shows how to display details of an AVC profile:

```
> show avc profile detailed
Application-Name                  Application-Group-Name          Action   DSCP
=====
ftp                               file-sharing                   Drop     -
flash-video                       browsing                       Mark     10
facebook                         browsing                       Mark     10

Associated WLAN IDs               :
Associated Remote LAN IDs         :
Associated Guest LAN IDs          :
```

Related Commands

config avc profile delete
config avc profile create
config avc profile rule
config wlan avc
show avc profile
show avc applications
show avc statistics
debug avc error
debug avc events

show avc statistics application

To display the statistics of an application, use the **show avc statistics application** command.

show avc statistics application *application_name* **top-users** [**downstream wlan** | **upstream wlan** | **wlan**] [*wlan_id*]}

Syntax Description

<i>application_name</i>	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-users	Displays AVC statistics for top application users.
downstream	(Optional) Displays statistics of top downstream applications.
wlan	(Optional) Displays AVC statistics of a WLAN.
<i>wlan_id</i>	WLAN identifier from 1 to 512.
upstream	(Optional) Displays statistics of top upstream applications.

Command Default

None.

Examples

This example shows how to display the AVC statistics of the top clients in WLAN 1 that use FTP as the downstream application:

> **show avc statistics application ftp top-users downstream wlan 1**

Client MAC Bytes (Up/Down) (Total)	DSCP In Out	Client IP	WLAN ID	Packets (n secs)	Bytes (n secs)	Avg Pkt Size	Packets (Total)
=====	=====	=====	=====	=====	=====	=====	=====
00:0a:ab:15:00:9c (U)	338 0 0	172.16.31.156	1	16	91	5	43
		(D) 172.16.31.156	1	22	5911	268	48
6409 0 0							
00:0a:ab:15:00:5a (U)	84 0 0	172.16.31.90	1	7	39	5	13
		(D) 172.16.31.90	1	12	5723	476	18
5869 0 0							
00:0a:ab:15:00:60 (U)	8666 0 0	172.16.31.96	1	19	117	6	75
		(D) 172.16.31.96	1	19	4433	233	83
9595 0 0							
00:0a:ab:15:00:a4 (U)	161 0 0	172.16.31.164	1	18	139	7	21
		(D) 172.16.31.164	1	23	4409	191	24
4439 0 0							
00:0a:ab:15:00:48 (U)	2738 0 0	172.16.31.72	1	21	2738	130	21
		(D) 172.16.31.72	1	22	4367	198	22
4367 0 0							
00:0a:ab:15:00:87 (U)	301 0 0	172.16.31.135	1	11	47	4	49

7755	0	0	(D)	172.16.31.135	1	12	4208	350	48
00:0a:ab:15:00:92	(U)	172.16.31.146	1	10	73	7	11		
84	0	0							
			(D)	172.16.31.146	1	9	4168	463	11
4201	0	0							
00:0a:ab:15:00:31	(U)	172.16.31.49	1	11	95	8	34		
250	0	0							
			(D)	172.16.31.49	1	18	3201	177	43
3755	0	0							
00:0a:ab:15:00:46	(U)	172.16.31.70	1	7	47	6	20		
175	0	0							
			(D)	172.16.31.70	1	10	3162	316	23
3448	0	0							
00:0a:ab:15:00:b3	(U)	172.16.31.179	1	10	85	8	34		
241	0	0							

Related Commands

config avc profile delete
config avc profile create
config avc profile rule
config wlan avc
show avc profile
show avc applications
show avc statistics client
show avc statistics wlan
show avc statistics top-apps
show avc statistics guest-lan
show avc statistics remote-lan
debug avc error
debug avc events

show avc statistics client

To display the client Application Visibility and Control (AVC) statistics, use the **show avc statistics client** command.

show avc statistics client *client_MAC* {**application** *application_name* | **top-apps** [**upstream** | **downstream**]}

Syntax Description

<i>client_MAC</i>	MAC address of the client.
application	Displays AVC statistics for an application.
<i>application_name</i>	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-apps	Displays AVC statistics for top applications.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.

Command Default

None.

Examples

This example shows how to display the AVC statistics of an application for a client:

```
> show avc statistics client 00:0a:ab:15:00:01 application http
Description                               Upstream      Downstream
=====
Number of Packtes(n secs)                 5059          6369
Number of Bytes(n secs)                   170144        8655115
Average Packet size(n secs)                33           1358
Total Number of Packtes                    131878        150169
Total Number of Bytes                     6054464       205239972
DSCP Incoming packet                      16             0
DSCP Outgoing Packet                      16             0
```

This example shows how to display the AVC statistics of the top applications for a client:

```
> show avc statistics client 00:0a:ab:15:00:01 top-apps
Application-Name      Packets   Bytes    Avg Pkt  Packets   Bytes    DSCP  DSCP
  (Up/Down)  (n secs) (n secs)  Size     (Total)  (Total)  In    Out
=====
http          (U)    6035    637728    105      6035    637728    16    16
              (D)    5420    7218796   1331     5420    7218796     0     0
gpp           (U)    1331    1362944   1024     1331    1362944     0     0
              (D)     0         0         0         0         0     0     0
smp           (U)    1046    1071104   1024     1046    1071104     0     0
              (D)     0         0         0         0         0     0     0
```

vrrp	(U)	205	209920	1024	205	209920	0	0
	(D)	0	0	0	0	0	0	0
bittorrent	(U)	117	1604	13	117	1604	0	0
	(D)	121	70469	582	121	70469	0	0
icmp	(U)	0	0	0	0	0	0	0
	(D)	72	40032	556	72	40032	48	48
edonkey	(U)	112	4620	41	112	4620	0	0
	(D)	105	33076	315	105	33076	0	0
dns	(U)	10	380	38	10	380	0	0
	(D)	7	1743	249	7	1743	0	0
realmedia	(U)	2	158	79	2	158	24	24
	(D)	2	65	32	2	65	0	0

Related Commands

config avc profile delete
config avc profile create
config avc profile rule
config wlan avc
show avc profile
show avc applications
show avc statistics applications
show avc statistics wlan
show avc statistics top-apps
show avc statistics guest-lan
show avc statistics remote-lan
debug avc error
debug avc events

show avc statistics guest-lan

To display the Application Visibility and Control (AVC) statistics of a guest LAN, use the **show avc statistics guest-lan** command.

show avc statistics guest-lan *guest-lan_id* {**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}

Syntax Description

<i>guest-lan_id</i>	Guest LAN identifier from 1 to 5.
application	Displays AVC statistics for an application.
<i>application_name</i>	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-app-groups	Displays AVC statistics for top application groups.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.
top-apps	Displays AVC statistics for top applications.

Command Default

None.

Examples

This example shows how to display the AVC statistics of a guest LAN:

```
> show avc statistics guest-lan 1
Application-Name      Packets   Bytes   Avg Pkt   Packets   Bytes
      (Up/Down)      (n secs) (n secs) Size      (Total)   (Total)
=====
unclassified          (U) 191464   208627    1      92208613 11138796586
                      (D) 63427   53440610 842     16295621 9657054635
ftp                   (U) 805      72880     90      172939   11206202
                      (D) 911      58143     63      190900   17418653
http                  (U) 264904   12508288  47      27493945 2837672192
                      (D) 319894   436915253 1365    29850934 36817587924
gre                   (U) 0         0         0      10158872 10402684928
                      (D) 0         0         0         0         0
icmp                  (U) 1         40        40       323      98476
                      (D) 7262    4034576   555     2888266 1605133372
ipinip                (U) 62565    64066560 1024    11992305 12280120320
                      (D) 0         0         0         0         0
imap                  (U) 1430     16798     11      305161   3795766
                      (D) 1555     576371    370     332290   125799465
irc                   (U) 9         74        8       1736     9133
                      (D) 11        371       33      1972     173381
nntp                  (U) 22        158       7       1705     9612
                      (D) 22        372      16      2047     214391
```

Related Commands

config avc profile delete

config avc profile create
config avc profile rule
config wlan avc
show avc profile
show avc applications
show avc statistics client
show avc statistics wlan
show avc statistics top-apps
show avc statistics applications
show avc statistics remote-lan
debug avc error
debug avc events

show avc statistics remote-lan

To display the Application Visibility and Control (AVC) statistics of a remote LAN, use the **show avc statistics remote-lan** command.

show avc statistics remote-lan *remote-lan_id*{**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}

Syntax Description

<i>remote-lan_id</i>	Remote LAN identifier from 1 to 512.
application	Displays AVC statistics for an application.
<i>application_name</i>	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-app-groups	Displays AVC statistics for top application groups.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.
top-apps	Displays AVC statistics for top applications.

Command Default

None.

Examples

This example shows how to display the AVC statistics of a remote LAN:

```
> show avc statistics remote-lan 1
Application-Name      Packets   Bytes   Avg Pkt   Packets   Bytes
      (Up/Down)      (n secs) (n secs) Size      (Total)   (Total)
=====
unclassified          (U) 191464 208627    1      92208613 11138796586
                    (D) 63427 53440610 842     16295621 9657054635
ftp                   (U) 805    72880    90      172939   11206202
                    (D) 911    58143    63      190900   17418653
http                  (U) 264904 12508288 47      27493945 2837672192
                    (D) 319894 436915253 1365    29850934 36817587924
gre                   (U) 0       0        0      10158872 10402684928
                    (D) 0       0        0        0         0
icmp                  (U) 1       40       40      323      98476
                    (D) 7262   4034576 555     2888266 1605133372
ipinip                (U) 62565  64066560 1024    11992305 12280120320
                    (D) 0       0        0        0         0
imap                  (U) 1430   16798    11      305161   3795766
                    (D) 1555   576371  370     332290  125799465
irc                   (U) 9       74       8       1736     9133
                    (D) 11      371     33      1972    173381
nntp                  (U) 22     158      7       1705     9612
                    (D) 22     372     16      2047    214391
```

Related Commands

config avc profile delete

config avc profile create
config avc profile rule
config wlan avc
show avc profile
show avc applications
show avc statistics client
show avc statistics wlan
show avc statistics top-apps
show avc statistics guest-lan
show avc statistics applications
debug avc error
debug avc events

show avc statistics top-apps

To display the Application Visibility and Control (AVC) statistics for the top applications, use the **show avc statistics top-apps** command.

show avc statistics top-apps[upstream | downstream]

Syntax Description

upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.

Command Default

None.

Examples

This example shows how to display the AVC statistics for the top applications:

```
> show avc statistics top-apps
Application-Name          Packets      Bytes      Avg Pkt      Packets      Bytes
  (Up/Down)              (n secs)    (n secs)    Size         (Total)      (Total)
=====
http                      (U)    204570    10610912      51    28272539    2882294016
                        (D)    240936    327624221    1359    30750570    38026889010
realmedia                 (U)       908       62154        68      400698      26470359
                        (D)   166694   220522943    1322    35802836    47131836785
mpls-in-ip               (U)    77448    79306752    1024    10292787    10539813888
                        (D)         0         0         0         0         0
fire                     (U)    70890    72591360    1024    10242484    10488303616
                        (D)         0         0         0         0         0
pipe                     (U)    68296    69935104    1024    10224255    10469637120
                        (D)         0         0         0         0         0
gre                       (U)    60982    62445568    1024    10340221    10588386304
                        (D)         0         0         0         0         0
crudp                    (U)    26430    27064320    1024    10109812    10352447488
                        (D)         0         0         0         0         0
rtp                       (U)         0         0         0         0         0
                        (D)     7482    9936096    1328    2603923     3458009744
icmp                     (U)         0         0         0        323        98476
                        (D)    10155    5640504     555    2924693    1625363564
```

Related Commands

config avc profile delete
config avc profile create
config avc profile rule
config wlan avc
show avc profile
show avc applications
show avc statistics client
show avc statistics wlan
show avc statistics applications
show avc statistics guest-lan

show avc statistics remote-lan

debug avc error

debug avc events

show avc statistics wlan

To display the Application Visibility and Control (AVC) statistics of a WLAN, use the **show avc statistics wlan** command.

show avc statistics wlan *wlan_id* {**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}

Syntax Description

<i>wlan_id</i>	WLAN identifier from 1 to 512.
application	Displays AVC statistics for an application.
<i>application_name</i>	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-app-groups	Displays AVC statistics for top application groups.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.
top-apps	Displays AVC statistics for top applications.

Command Default

None.

Examples

This example shows how to display the AVC statistics of a WLAN:

```
> show avc statistics wlan 1
Application-Name      Packets   Bytes   Avg Pkt   Packets   Bytes
      (Up/Down)      (n secs) (n secs)  Size      (Total)   (Total)
=====
unclassified          (U) 191464   208627    1      92208613 11138796586
                    (D) 63427   53440610 842     16295621 9657054635
ftp                   (U) 805      72880     90      172939   11206202
                    (D) 911      58143     63      190900   17418653
http                  (U) 264904   12508288 47      27493945 2837672192
                    (D) 319894   436915253 1365    29850934 36817587924
gre                   (U) 0         0         0      10158872 10402684928
                    (D) 0         0         0         0         0
icmp                  (U) 1         40        40      323      98476
                    (D) 7262     4034576   555     2888266 1605133372
ipinip                (U) 62565    64066560 1024    11992305 12280120320
                    (D) 0         0         0         0         0
imap                  (U) 1430     16798     11      305161   3795766
                    (D) 1555     576371    370     332290   125799465
irc                   (U) 9         74        8       1736     9133
                    (D) 11        371       33      1972     173381
nntp                  (U) 22        158       7       1705     9612
                    (D) 22        372      16      2047     214391
```

This example shows how to display the AVC statistics of an FTP application for a WLAN:

```
> show avc statistics wlan 1 application ftp
Description      Upstream   Downstream
=====

```

Number of Packtes(n secs)	0	0
Number of Bytes(n secs)	0	0
Average Packet size(n secs)	0	0
Total Number of Packtes	32459	64888
Total Number of Bytes	274	94673983

Related Commands

- config avc profile delete**
- config avc profile create**
- config avc profile rule**
- config wlan avc**
- show avc profile**
- show avc applications**
- show avc statistics client**
- show avc statistics applications**
- show avc statistics top-apps**
- show avc statistics guest-lan**
- show avc statistics remote-lan**
- debug avc error**
- debug avc events**

Show CAC Commands

Use the **show cac** commands to display Call Admission Control (CAC) voice and video summary and statistics.

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.

Examples

This example shows how to view the detailed voice CAC statistics for the 802.11b radio:

```
> 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 insufficient bw.... 0
  Num of Calls Rejected due to invalid params.... 0
  Num of Calls Rejected due to PHY rate..... 0
  Num of Calls Rejected due to QoS policy..... 0
SIP CAC Call Stats
  Total Num of Calls in progress..... 0
  Num of 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 Commands

config 802.11 cac voice
config 802.11 cac defaults
config 802.11 cac defaults
config 802.11 cac video
config 802.11 cac multimedia

show cac voice summary

show cac video stats

show cac video summary

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.

Examples This example shows how to display the list of all APs with brief voice statistics:

```
> 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 Commands **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.

Examples

This example shows how to view the detailed video CAC statistics for the 802.11b radio:

```
> 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 insufficient bw.... 0
  Num of Calls Rejected due to invalid params.... 0
  Num of Calls Rejected due to PHY rate..... 0
  Num of Calls Rejected due to QoS policy..... 0
SIP CAC Call Stats
  Total Num of Calls in progress..... 0
  Num of 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.

Examples

This example shows how to display the list of all access points with brief video statistics:

```
> 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 Client Commands

Use the **show client** commands to see client settings.

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	Displays active calls.
rejected	Displays 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.

Examples

This example shows how to display the active client calls on an 802.11a network:

```
> show client calls active 802.11a
Client MAC          Username          Total Call
                   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 Commands

debug voice-diag

show client roam-history

To display the roaming history of a specified client, use the **show client roam-history** command.

show client roam-history *mac_address*

Syntax	Description

<i>mac_address</i>	Client MAC address.

Command Default

None.

Examples

This example shows how to display the roaming history of a specified client:

```
> show client roam-history 00:14:6c:0a:57:77
```

show client summary

To display a summary of clients associated with a Cisco lightweight access point, use the **show client summary** command.

show client summary

Syntax Description This command has no arguments or keywords.

Command Default None.

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 (blacklisted).

Examples This example shows how to display a summary of the active clients:

```
> 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
```

Related Commands **show client summary guest-lan**

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.

Examples This example shows how to display a summary of the active wired guest LAN clients:

```
> 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.
<i>client_mac</i>	MAC address of the client.
<i>ap_mac</i>	MAC address of the tsm access point.
all	Specifies the list of all access points to which the client has associations.

Command Default

None.

Examples

This example shows how to display the client's TSM for the 802.11a network:

```
> 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

<i>username</i>	Client's username.

Command Default

None.

Examples

This example shows how to display the detailed information for a client by name:

```
> show client username IT_007
MAC Address      AP ID   Status      WLAN Id   Authenticated
-----
xx:xx:xx:xx:xx:xx  1      Associated   1         No
```

Related Commands

show client ap
show client detail
show client summary

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 the last 3 roaming history. The output contains the Timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, reason for roaming-failure.
rssi	Displays the client's RSSI values in the last 5 seconds when voice diagnostics are enabled.
status	Displays status of voice diagnostics for clients.
tspec	Displays TSPEC for voice diagnostic clients.

Command Default

None.

Examples

This example shows how to display the status of voice diagnostics for clients:

```
> show client voice-diag status
Voice Diagnostics Status: FALSE
```

Related Commands

show client ap
show client detail
show client summary
debug voice-diag

show flow exporter

To display the details or the statistics of the flow exporter, use the **show flow exporter** command.

show flow exporter {summary | statistics}

Syntax Description

summary	Displays summary of flow exporter.
statistics	Displays the statistics of flow exporters such as number of records sent, time when the last record was sent.

Command Default

None.

Examples

This example shows how to display the flow exporter details:

```
> show flow exporter summary
Exporter-Name      Exporter-IP      Port
=====
expol              9.9.120.115     800
```

Related Commands

show flow monitor
config flow
config wlan flow

show flow monitor summary

To display the details of the NetFlow monitor, use the **show flow monitor summary** command.

Syntax Description This command has no arguments or keywords.

Command Default None.

Usage Guidelines Netflow record monitoring and export are used for integration with an NMS or any Netflow analysis tool.

Examples This example shows how to display the details of the NetFlow monitor:

```
> show flow monitor summary
Monitor-Name      Exporter-Name      Exporter-IP      Port  Record Name
=====
mon1              expol              9.9.120.115      800
ipv4_client_app_flow_record
```

Related Commands

- show flow exporter**
- config flow**
- config wlan flow**

Show mDNS Commands

Use the **show mdns** commands to display information about Multicast DNS (mDNS).

show mdns profile

To display mDNS profile information, use the **show mdns profile** command.

show mdns profile {**summary** | **detailed** *profile-name*}

Syntax Description

summary	Displays the summary of the mDNS profiles.
detailed	Displays details of an mDNS profile.
<i>profile-name</i>	Name of the mDNS profile.

Command Default

None.

Examples

This example shows how to display the summary of all the mDNS profiles:

```
> show mdns profile summary
Number of Profiles..... 2

ProfileName                No. Of Services
-----
default-mdns-profile      5
profile1                  2
```

This example shows how to display the detailed information of an mDNS profile:

```
> show mdns profile detailed default-mdns-profile

Profile Name..... default-mdns-profile
Profile Id..... 1
No of Services..... 5
Services..... AirPrint
               AppleTV
               HP_Photosmart_Printer_1
               HP_Photosmart_Printer_2
               Printer

No. Interfaces Attached..... 0
No. Interface Groups Attached..... 0
No. Wlans Attached..... 1
Wlan Ids..... 1
```

Related Commands

config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile

config wlan mdns
config mdns profile
show mnds service
clear mdns service-database
debug mdns all
debug mdns error
debug mdns detail
debug mdns message

show mnds service

To display mDNS service information, use the **show mnds service** command.

show mnds service {**summary** | **detailed** *service-name*}

Syntax Description

summary	Displays the summary of all mDNS services.
detailed	Displays details of an mDNS service.
<i>service-name</i>	Name of the mDNS service.

Command Default

None.

Examples

This example shows how to display the summary of the mDNS services:

```
> show mnds service summary
Number of Services..... 5

Service-Name                Service-string
-----
AirPrint                    _ipp._tcp.local.
AppleTV                    _airplay._tcp.local.
HP_Photosmart_Printer_1    _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2    _cups._sub._ipp._tcp.local.
Printer                    _printer._tcp.local.
```

This example shows how to display the details of an mDNS service:

```
> show mnds service detailed AirPrint
Service Name..... AirPrint
Service Id..... 1
Service query status..... Enabled
Number of Profiles..... 2
Profile..... student-profile
                    guest-profile

Number of Service Providers ..... 2
Service Provider    MAC-Address      VLAN    Type
-----
user1               60:33:4b:2b:a6:9a    104     Wired
laptopa             00:21:1b:ea:36:60    105     Wireless
```

Related Commands

config mnds query interval
config mnds service
config mnds snooping
config interface mnds-profile
config interface group mnds-profile
config wlan mnds

show mdns profile
config mdns profile
clear mdns service-database
debug mdns all
debug mdns error
debug mdns detail
debug mdns message

Show Radio Frequency ID Commands

Use the **show rfid** commands to display radio frequency ID settings.

show rfid client

To display the radio frequency identification (RFID) tags that are associated to the controller as clients, use the **show rfid client** command.

show rfid client

Syntax Description This command has no arguments or keywords.

Command Default None.

Usage Guidelines When the RFID tag is not in client mode, the above fields are blank.

Examples This example shows how to display the RFID tag that is associated to the controller as clients:

```
> show rfid client
-----
RFID Mac          VENDOR      Heard      Associated AP      Chnl      Client State
-----
00:14:7e:00:0b:b1 Pango        35         AP0019.e75c.fef4   1         Probing
```

Related Commands

- config rfid status
- config rfid timeout
- show rfid config
- show rfid detail
- show rfid summary

show rfid config

To display the current radio frequency identification (RFID) configuration settings, use the **show rfid config** command.

show rfid config

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the current RFID configuration settings:

```
> show rfid config
RFID Tag Data Collection ..... Enabled
RFID Tag Auto-Timeout ..... Enabled
RFID Client Data Collection ..... Disabled
RFID Data Timeout ..... 200 seconds
```

Related Commands

- config rfid status
- config rfid timeout
- show rfid client
- show rfid detail
- show rfid summary

show rfid detail

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

show rfid detail *mac_address*

Syntax Description

<i>mac_address</i>	MAC address of an RFID tag.

Command Default

None.

Examples

This example shows how to display detailed RFID information:

```
> show rfid detail 00:12:b8:00:20:52
RFID address..... 00:12:b8:00:20:52
Vendor..... G2
Last Heard..... 51 seconds ago
Packets Received..... 2
Bytes Received..... 324
Cisco Type.....
Content Header
=====
Version..... 0
Tx Power..... 12 dBm
Channel..... 1
Reg Class..... 12
Burst Length..... 1
CCX Payload
=====
Last Sequence Control..... 0
Payload length..... 127
Last Sequence Control..... 0
Payload length..... 127
Payload Data Hex Dump
01 09 00 00 00 00 0b 85 52 52 52 02 07 4b ff ff
7f ff ff ff 03 14 00 12 7b 10 48 53 c1 f7 51 4b
50 ba 5b 97 27 80 00 67 00 01 03 05 01 42 34 00
00 03 05 02 42 5c 00 00 03 05 03 42 82 00 00 03
05 04 42 96 00 00 03 05 05 00 00 00 55 03 05 06
42 be 00 00 03 02 07 05 03 12 08 10 00 01 02 03
04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 03 0d 09 03
08 05 07 a8 02 00 10 00 23 b2 4e 03 02 0a 03
Nearby AP Statistics:
lap1242-2(slot 0, chan 1) 50 seconds ag.... -76 dBm
lap1242(slot 0, chan 1) 50 seconds ago..... -65 dBm
```

Related Commands

config rfid status
config rfid timeout
show rfid config
show rfid client
show rfid summary

show rfid summary

To display a summary of the radio frequency identification (RFID) information for a specified tag, use the **show rfid summary** command.

show rfid summary

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display a summary of RFID information:

```
> show rfid summary
Total Number of RFID : 5
```

RFID ID	VENDOR	Closest AP	RSSI	Time Since Last Heard
00:04:f1:00:00:04	Wherenet	ap:1120	-51	858 seconds ago
00:0c:cc:5c:06:d3	Aerosct	ap:1120	-51	68 seconds ago
00:0c:cc:5c:08:45	Aerosct	AP_1130	-54	477 seconds ago
00:0c:cc:5c:08:4b	Aerosct	wolverine	-54	332 seconds ago
00:0c:cc:5c:08:52	Aerosct	ap:1120	-51	699 seconds ago

Related Commands

- config rfid status**
- config rfid timeout**
- show rfid client**
- show rfid detail**
- show rfid config**

Other Show Commands

This section lists the other **show** commands to display controller settings.

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.
<i>cisco_ap</i>	Access point name.

Command Default

None.

Examples

This example shows how to display AP channel utilization metrics of the AP myAP1:

```
> 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.
<i>mac_address</i>	MAC address of the client.

Command Default

None.

Examples

This example shows how to display 802.11b Layer 2 client roaming information:

```
> 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
```

Related Commands

config 802.11 l2roam rf-params

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.

Examples	This example shows how to display the disassociated clients after a handoff:

```
> show advanced send-disassoc-on-handoff
Send Disassociate on Handoff..... Disabled
```


show advanced sip-preferred-call-no

To display the list of preferred call numbers, use the **show advanced sip-preferred-call-no** command.

show advanced sip-preferred-call-no

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the list of preferred call numbers:

```
> show advanced sip-preferred-call-no
Preferred Call Numbers List
Call Index      Preferred Call No
-----
1               911
2               100
3               101
4               102
5               103
6               104
```

show advanced sip-snooping-ports

To display the port range for call snooping, use the **show advanced sip-snooping-ports** command.

show advanced sip-snooping-ports

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the call snooping port range:

```
> show advanced sip-snooping-ports
SIP Call Snoop Ports: 1000 - 2000
```

Related Commands

- show cac voice stats**
- show cac voice summary**
- show cac video stats**
- show cac video summary**
- config 802.11 cac video sip**
- config 802.11 cac voice sip**
- show advanced sip-preferred-call-no**
- config advanced sip-snooping-ports**
- debug cac**

show arp kernel

To display the kernel Address Resolution Protocol (ARP) cache information, use the **show arp kernel** command.

show arp kernel

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display kernel ARP cache information:

```
> show arp kernel
IP address      HW type      Flags        HW address    Mask         Device
192.0.2.1       0x1          0x2          00:1A:6C:2A:09:C2  *           dt10
192.0.2.8       0x1          0x6          00:1E:E5:E6:DB:56  *           dt10
```

Related Commands

- clear arp**
- debug arp**
- show route kernel**

show arp switch

To display the Cisco wireless LAN controller MAC addresses, IP addresses, and port types, use the **show arp switch** command.

show arp switch

Syntax Description

This command has no arguments or keywords.

Examples

This example shows how to display Address Resolution Protocol (ARP) cache information for the switch:

```
> show arp switch
MAC Address      IP Address      Port      VLAN      Type
-----
xx:xx:xx:xx:xx:xx  xxx.xxx.xxx.xxx  service port  1
xx:xx:xx:xx:xx:xx  xxx.xxx.xxx.xxx  service port
xx:xx:xx:xx:xx:xx  xxx.xxx.xxx.xxx  service port
```

Related Commands

clear arp

debug arp

show arp kernel

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.

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.

Examples	This example shows how to display the default boot image information:

```
> 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.

Examples This example shows how to display band selection information:

```
> 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.

Examples This example shows how to display buffer information of the 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 cdp

To display the status of Cisco Discovery Protocol (CDP) and view the details of the CDP protocol, 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	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.

Examples

This example shows how to display the CDP traffic information:

```
> 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 lsc

To verify that the controller has generated a Locally Significant Certificate (LSC), use the **show certificate lsc summary** command.

show certificate lsc {summary | ap-provision}

Syntax Description

summary	Displays a summary of LSC certificate settings and certificates.
ap-provision	Displays details about the access points that are provisioned using the LSC.

Command Default

None.

Examples

This example shows how to display a summary of the LSC:

```
> show certificate lsc summary
LSC Enabled..... Yes
LSC CA-Server..... http://10.0.0.1:8080/caserver
LSC AP-Provisioning..... Yes
Provision-List..... Not Configured
LSC Revert Count in AP reboots..... 3
LSC Params:
Country..... 4
State..... ca
City..... ss
Orgn..... org
Dept..... dep
Email..... dep@co.com
KeySize..... 390
LSC Certs:
CA Cert..... Not Configured
RA Cert..... Not Configured
```

This example shows how to display the details about the access points that are provisioned using the LSC:

```
> show certificate lsc ap-provision
LSC AP-Provisioning..... Yes
Provision-List..... Present
Idx Mac Address
---
1 00:18:74:c7:c0:90
```

Related Commands

config certificate lsc
show certificate compatibility
config certificate
show certificate summary
show local-auth certificates

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.

Examples

This example shows how to display the SSC:

```
> 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 Commands

show certificate ssc
show mobility group member
config certificate ssc
config mobility group member hash

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.

Examples This example shows how to display a summary of the certificate:

```
> show certificate summary
Web Administration Certificate..... Locally Generated
Web Authentication Certificate..... Locally Generated
Certificate compatibility mode:..... off
```

Related Commands

- config certificate**
- config certificate lsc**
- show certificate lsc**
- show certificate compatibility**
- show local-auth certificate**

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.

Examples	This example shows how to display the core dump summary:

```
> 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.

Examples

This example shows how to display the current CPU usage information:

```
> show cpu  
Current CPU load: 2.50%
```

show custom-web

To display web authentication customization information, use the **show custom-web** command.

show custom-web

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the web authentication customization information:

```
> show custom-web
Radius Authentication Method..... PAP
Cisco Logo..... Enabled
CustomLogo..... None
Custom Title..... None
Custom Message..... None
Custom Redirect URL..... None
External web authentication Mode..... Disabled
External web authentication URL..... None
```

Related Commands

- config custom-web weblogo**
- config custom-web webmessage**
- config custom-web webtitle**
- config custom-web weblogo**
- config custom-web ext-webauth-mode**
- config custom-web redirectUrl**
- config custom-web ext-webauth-type**
- config custom-web ext-webauth-url**
- show custom-web**

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.

Examples	This example shows how to display a summary of the local database configuration:

```
> show database summary
Maximum Database Entries..... 2048
Maximum Database Entries On Next Reboot..... 2048
Database Contents
  MAC Filter Entries..... 2
  Exclusion List Entries..... 0
  AP Authorization List Entries..... 1
  Management Users..... 1
  Local Network Users..... 1
    Local Users..... 1
    Guest Users..... 0
  Total..... 5
```

Related Commands	config database size

show dhcp

To display the internal Dynamic Host Configuration Protocol (DHCP) server configuration, use the **show dhcp** command.

show dhcp {leases | summary | scope}

Syntax Description

leases	Displays allocated DHCP leases.
summary	Displays DHCP summary information.
<i>scope</i>	Name of a scope to display the DHCP information for that scope.

Command Default

None.

Examples

This example shows how to display the allocated DHCP leases:

```
> show dhcp leases
No leases allocated.
```

This example shows how to display the DHCP summary information:

```
> show dhcp summary
Scope Name      Enabled      Address Range
003             No           0.0.0.0 -> 0.0.0.0
```

This example shows how to display the DHCP information for the scope 003:

```
> show dhcp 003
Enabled..... No
Lease Time..... 0
Pool Start..... 0.0.0.0
Pool End..... 0.0.0.0
Network..... 0.0.0.0
Netmask..... 0.0.0.0
Default Routers..... 0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain.....
DNS..... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers..... 0.0.0.0 0.0.0.0 0.0.0.0
```

Related Commands

config dhcp proxy
config dhcp timeout
config interface dhcp
config wlan dhcp server
debug dhcp
debug dhcp service-port


```
debug disable-all  
config dhcp  
show dhcp proxy
```

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.

Examples This example shows how to display the established DTLS connections:

```
> show dtls connections
AP Name      Local Port  Peer IP      Peer Port    Ciphersuite
-----
1130         Capwap_Ctrl 1.100.163.210 23678        TLS_RSA_WITH_AES_128_CBC_SHA
1130         Capwap_Data 1.100.163.210 23678        TLS_RSA_WITH_AES_128_CBC_SHA
1240         Capwap_Ctrl 1.100.163.209 59674        TLS_RSA_WITH_AES_128_CBC_SHA
```

show dhcp proxy

To display the status of DHCP proxy handling, use the **show dhcp proxy** command.

show dhcp proxy

Syntax Description	This command has no arguments or keywords.

Command Default	None.

Examples	This example shows how to display the status of DHCP proxy information:

```
> show dhcp proxy
DHCP Proxy Behavior: enabled
```

Related Commands	config dhcp proxy config dhcp timeout config interface dhcp config wlan dhcp_server debug dhcp debug dhcp service-port debug disable-all show dhcp config dhcp

show dhcp timeout

To display the DHCP timeout value, use the **show dhcp timeout** command.

show dhcp timeout

Syntax Description	This command has no arguments or keywords.

Command Default	None.

Examples	This example shows how to display the DHCP timeout value:

```
> show dhcp timeout
DHCP Timeout (seconds) ..... 10
```

Related Commands	config dhcp proxy config dhcp config interface dhcp config wlan dhcp_server debug dhcp debug dhcp service-port debug disable-all show dhcp show dhcp proxy

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

<i>guest_lan_id</i>	ID of selected wired guest LAN.

Command Default

None.

Usage Guidelines

To display all wired guest LANs configured on the controller, use the **show guest-lan summary** command.

Examples

This example shows how to display the guest LAN configuration:

```
> 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
```

Related Commands

config guest-lan
config guest-lan custom-web ext-webauth-url
config guest-lan custom-web global disable
config guest-lan custom-web login_page
config guest-lan nac
config guest-lan security

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.

Usage Guidelines You can execute this command only before the **clear config** or **save config** command.

Examples This example shows how to display a list of any ignored commands or invalid configuration values in a configuration file:

```
> 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.

Usage Guidelines

Some wireless LAN controllers may have no crypto accelerator (VPN termination module) or power supplies listed because they have no provisions for VPN termination modules or power supplies.

Examples

This example shows how to display a physical inventory of the controller:

```
> show inventory
Switch Description..... Cisco Controller
Machine Model..... WLC4404-100
Serial Number..... FLS0923003B
Burned-in MAC Address..... 00:0B:85:32:AB:60
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK
```

Related Commands

show ap inventory

show license agent

To display the license agent counter and session information on the Cisco 5500 Series Controller, use the **show license agent** command.

show license agent {counters | sessions}

Syntax Description

counters	Displays license agent counter information.
sessions	Displays session information.

Command Default

None.

Examples

This example shows how to display the license agent counters information:

```
> show license agent counters
License Agent Counters
Request Messages Received:0: Messages with Errors:0
Request Operations Received:0: Operations with Errors:0
Notification Messages Sent:0: Transmission Errors:0: Soap Errors:0
```

This example shows how to display the license agent sessions information:

```
> show license agent sessions
License Agent Sessions: 0 open, maximum is 9
```

Related Commands

config license agent
clear license agent
show license all
show license detail
show license feature
show license image-level
show license summary

show license all

To display information for all licenses on the Cisco 5500 Series Controller, use the **show license all** command.

show license all

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display all the licenses:

```
> show license all
License Store: Primary License Storage
StoreIndex: 0 Feature: wplus-ap-count Version: 1.0
  License Type: Permanent
  License State: Inactive
  License Count: 12/0/0
  License Priority: Medium
StoreIndex: 1 Feature: base Version: 1.0
  License Type: Permanent
  License State: Active, Not in Use
  License Count: Non-Counted
  License Priority: Medium
StoreIndex: 2 Feature: wplus Version: 1.0
  License Type: Permanent
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Medium
License Store: Evaluation License Storage
StoreIndex: 0 Feature: wplus Version: 1.0
  License Type: Evaluation
  License State: Inactive
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 6 weeks 6 days
  License Count: Non-Counted
  License Priority: Low
StoreIndex: 1 Feature: wplus-ap-count Version: 1.0
  License Type: Evaluation
  License State: Active, In Use
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 2 weeks 3 days
    Expiry date: Thu Jun 25 18:09:43 2009
  License Count: 250/250/0
  License Priority: High
StoreIndex: 2 Feature: base Version: 1.0
  License Type: Evaluation
  License State: Inactive
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 8 weeks 4 days
  License Count: Non-Counted
  License Priority: Low
StoreIndex: 3 Feature: base-ap-count Version: 1.0
  License Type: Evaluation
  License State: Active, Not in Use, EULA accepted
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 8 weeks 3 days
  License Count: 250/0/0
  License Priority: Low
```

Related Commands

license install
show license agent
show license detail
show license feature
show license image-level
show license summary
license modify priority

show license capacity

To display the maximum number of access points allowed for this license on the Cisco 5500 Series Controller, the number of access points currently joined to the controller, and the number of access points that can still join the controller, use the **show license capacity** command.

show license capacity

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the license capacity:

```
> show license capacity
Licensed Feature    Max Count          Current Count      Remaining Count
-----
AP Count           250                47                 203
```

Related Commands

- license install
- show license all
- show license detail
- show license feature
- show license image-level
- show license summary
- license modify priority
- show license evaluation

show license detail

To display details of a specific license on the Cisco 5500 Series Controller, use the **show license detail** command.

show license detail *license-name*

Syntax Description

<i>license-name</i>	Name of a specific license.

Command Default

None.

Examples

This example shows how to display the license details:

```
> show license detail wplus
Feature: wplus          Period left: Life time
Index: 1      Feature: wplus  Version: 1.0
      License Type: Permanent
      License State: Active, In Use
      License Count: Non-Counted
      License Priority: Medium
      Store Index: 2
      Store Name: Primary License Storage
Index: 2      Feature: wplus  Version: 1.0
      License Type: Evaluation
      License State: Inactive
      Evaluation total period: 8 weeks 4 days
      Evaluation period left: 6 weeks 6 days
      License Count: Non-Counted
      License Priority: Low
      Store Index: 0
```

Related Commands

- license install**
- show license agent**
- show license all**
- show license feature**
- show license image-level**
- show license summary**
- license modify priority**

show license expiring

To display details of expiring licenses on the Cisco 5500 Series Controller, use the **show license expiring** command.

show license expiring

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the details of the expiring licenses:

```
> show license expiring
StoreIndex: 0 Feature: wplus Version: 1.0
  License Type: Evaluation
  License State: Inactive
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 6 weeks 6 days
  License Count: Non-Counted
  License Priority: Low
StoreIndex: 1 Feature: wplus-ap-count Version: 1.0
  License Type: Evaluation
  License State: Active, In Use
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 2 weeks 3 days
    Expiry date: Thu Jun 25 18:09:43 2009
  License Count: 250/250/0
  License Priority: High
StoreIndex: 2 Feature: base Version: 1.0
  License Type: Evaluation
  License State: Inactive
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 8 weeks 4 days
  License Count: Non-Counted
  License Priority: Low
StoreIndex: 3 Feature: base-ap-count Version: 1.0
  License Type: Evaluation
  License State: Active, Not in Use, EULA accepted
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 8 weeks 3 days
  License Count: 250/0/0
  License Priority: Low
```

Related Commands

- license install
- show license all
- show license detail
- show license in-use
- show license summary
- license modify priority
- show license evaluation

show license evaluation

To display details of evaluation licenses on the Cisco 5500 Series Controller, use the **show license evaluation** command.

show license evaluation

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the details of the evaluation licenses:

```
> show license evaluation
StoreIndex: 0 Feature: wplus Version: 1.0
  License Type: Evaluation
  License State: Inactive
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 6 weeks 6 days
  License Count: Non-Counted
  License Priority: Low
StoreIndex: 1 Feature: wplus-ap-count Version: 1.0
  License Type: Evaluation
  License State: Active, In Use
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 2 weeks 3 days
    Expiry date: Thu Jun 25 18:09:43 2009
  License Count: 250/250/0
  License Priority: High
StoreIndex: 2 Feature: base Version: 1.0
  License Type: Evaluation
  License State: Inactive
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 8 weeks 4 days
  License Count: Non-Counted
  License Priority: Low
StoreIndex: 3 Feature: base-ap-count Version: 1.0
  License Type: Evaluation
  License State: Active, Not in Use, EULA accepted
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 8 weeks 3 days
  License Count: 250/0/0
  License Priority: Low
```

Related Commands

- license install
- show license all
- show license detail
- show license expiring
- show license in-use
- show license summary
- license modify priority

show license feature

To display a summary of license-enabled features on the Cisco 5500 Series Controller, use the **show license feature** command.

show license feature

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the license-enabled features:

```
> show license feature
Feature name Enforcement Evaluation Clear Allowed Enabled
wplus          yes         yes         yes         yes
wplus-ap-count yes         yes         yes         yes
base           no          yes         yes         no
base-ap-count  yes         yes         yes         no
```

Related Commands

- license install**
- show license all**
- show license detail**
- show license expiring**
- show license image-level**
- show license in-use**
- show license summary**
- show license modify priority**
- show license evaluation**

show license file

To display a summary of license-enabled features on the Cisco 5500 Series Controller, use the **show license file** command.

show license file

Syntax Description

This command has no arguments or keywords.

Examples

This example shows how to display the license files:

```
> show license file
License Store: Primary License Storage
Store Index: 0
License: 11 wplus-ap-count 1.0 LONG NORMAL STANDALONE EXCL 12 KEYS INFINIT
E KEYS NEVER NEVER NiL SLM CODE CL_ND LCK NiL *1AR5NS7M5AD8PPU400
NiL NiL NiL 5 MINS <UDI><PID>AIR-CT5508-K9</PID><SN>RFD000P2D27<
/SN></UDI> Pe0L7tv8KDUqo:z1Pe423S5wasgM8G,tTs0i,7zLyA3VfxhnIe5aJa
m631R518JM3DPkr4O2DI43iLlKn7jomo3RF11LjMRqLkKhiLJ2tOyuftQSq2bCA06
nR3wIb38xKi3t$<WLC>AQEBIQAB//++mCzRUbOhw28vz0czAY0iAm7ocDLUMB9ER0
+BD3w2PhNEYwsBN/T3xXBqJqfC+oKRqWInXo3s+nsLU7rOtdOxoIxYZAo3LYmUJ+M
Fzsq1hKoJVlPyEvQ8H21MNUjVbhoN0gyIWsyiJaM8AQIkVBQFzhr10GYo1VzdzfJf
EPQIx6tZ++/Vtc/q3SF/5Ko8XCy=</WLC>
Comment:
Hash: iOGjuLlXgLhcTB113ohIzxVioHA=
. . .
```

Related Commands

- license install
- show license all
- show license detail
- show license expiring
- show license feature
- show license image-level
- show license in-use
- show license summary
- show license evaluation

show license handle

To display the license handles on the Cisco 5500 Series Controller, use the **show license handle** command.

show license handle

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the license handles:

```
> show license handle
Feature: wplus                               , Handle Count: 1
  Units: 01( 0), ID: 0x5e000001, NotifyPC: 0x1001e8f4 LS-Handle (0x00000001),
Units: ( 1)
  Registered clients: 1
    Context 0x1051b610, epID 0x10029378
Feature: base                               , Handle Count: 0
  Registered clients: 1
    Context 0x1053ace0, epID 0x10029378
Feature: wplus-ap-count                     , Handle Count: 1
  Units: 250( 0), ID: 0xd4000002, NotifyPC: 0x1001e8f4      LS-Handle (0x000
00002), Units: (250)
  Registered clients: None
Feature: base-ap-count                     , Handle Count: 0
  Registered clients: None
Global Registered clients: 2
    Context 0x10546270, epID 0x100294cc
    Context 0x1053bae8, epID 0x100294cc
```

Related Commands

- license install**
- show license all**
- show license detail**
- show license expiring**
- show license feature**
- show license image-level**
- show license in-use**
- show license summary**

show license image-level

To display the license image level that is in use on the Cisco 5500 Series Controller, use the **show license image-level** command.

show license image-level

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the image level license settings:

```
> show license image-level
Module name  Image level  Priority  Configured  Valid license
wnbu         wplus       1        YES        wplus
             base        2        NO
NOTE: wplus includes two additional features: Office Extend AP, Mesh AP.
```

Related Commands

- license install**
- show license all**
- show license detail**
- show license expiring**
- show license feature**
- license modify priority**
- show license in-use**
- show license summary**

show license in-use

To display the licenses that are in use on the Cisco 5500 Series Controller, use the **show license in-use** command.

show license in-use

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the licenses that are in use:

```
> show license in-use
StoreIndex: 2 Feature: wplus Version: 1.0
  License Type: Permanent
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Medium
StoreIndex: 1 Feature: wplus-ap-count Version: 1.0
  License Type: Evaluation
  License State: Active, In Use
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 2 weeks 3 days
    Expiry date: Thu Jun 25 18:09:43 2009
  License Count: 250/250/0
  License Priority: High
```

Related Commands

- license install
- show license all
- show license detail
- show license expiring
- show license feature
- show license image-level
- show license modify priority
- show license summary
- show license permanent
- show license evaluation

show license permanent

To display the permanent licenses on the Cisco 5500 Series Controller, use the **show license permanent** command.

show license permanent

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the permanent license's information:

```
> show license permanent
StoreIndex: 0 Feature: wplus-ap-count Version: 1.0
  License Type: Permanent
  License State: Inactive
  License Count: 12/0/0
  License Priority: Medium
StoreIndex: 1 Feature: base Version: 1.0
  License Type: Permanent
  License State: Active, Not in Use
  License Count: Non-Counted
  License Priority: Medium
StoreIndex: 2 Feature: wplus Version: 1.0
  License Type: Permanent
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Medium
```

Related Commands

- license install
- show license all
- show license detail
- show license expiring
- show license feature
- show license image-level
- show license in-use
- show license summary
- license modify priority
- show license evaluation

show license status

To display the license status on the Cisco 5500 Series Controller, use the **show license status** command.

show license status

Syntax Description	This command has no arguments or keywords.

Command Default	None.

Examples	This example shows how to display the license status:

```
> show license status
      License Type Supported
permanent  Non-expiring node locked license
extension  Expiring node locked license
evaluation  Expiring non node locked license
      License Operation Supported
install     Install license
clear       Clear license
annotate    Comment license
save        Save license
revoke      Revoke license
      Device status
Device Credential type: DEVICE
Device Credential Verification: PASS
Rehost Type: DC_OR_IC
```

Related Commands	license install show license all show license detail show license expiring show license feature show license image-level show license in-use show license summary license modify priority show license evaluation

show license statistics

To display license statistics on the Cisco 5500 Series Controller, use the **show license statistics** command.

show license statistics

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the license statistics:

```
> show license statistics
      Administrative statistics
Install success count:      0
Install failure count:     0
Install duplicate count:   0
Comment add count:         0
Comment delete count:      0
Clear count:               0
c   Save count:             0
    Save cred count:       0
      Client status
Request success count      2
Request failure count      0
Release count              0
Global Notify count       0
```

Related Commands

- license install
- show license all
- show license detail
- show license expiring
- show license feature
- show license image-level
- show license in-use
- show license summary
- license modify priority
- show license evaluation

show license summary

To display a brief summary of all licenses on the Cisco 5500 Series Controller, use the **show license summary** command.

show license summary

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display a brief summary of all licenses:

```
> show license summary
Index 1 Feature: wplus
      Period left: Life time
      License Type: Permanent
      License State: Active, In Use
      License Count: Non-Counted
      License Priority: Medium
Index 2 Feature: wplus-ap-count
      Period left: 2 weeks 3 days
      License Type: Evaluation
      License State: Active, In Use
      License Count: 250/250/0
      License Priority: High
Index 3 Feature: base
      Period left: Life time
      License Type: Permanent
      License State: Active, Not in Use
      License Count: Non-Counted
      License Priority: Medium
Index 4 Feature: base-ap-count
      Period left: 8 weeks 3 days
      License Type: Evaluation
      License State: Active, Not in Use, EULA accepted
      License Count: 250/0/0
      License Priority: Low
```

Related Commands

- license install**
- show license all**
- show license detail**
- show license expiring**
- show license feature**
- show license image-level**
- show license in-use**
- show license permanent**
- license modify priority**
- show license evaluation**

show license udi

To display unique device identifier (UDI) values for licenses on the Cisco 5500 Series Controller, use the **show license udi** command.

show license udi

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display the UDI values for licenses:

```
> show license udi
Device# PID                               SN                               UDI
-----
*0      AIR-CT5508-K9                     RFD000P2D27                     AIR-CT5508-K9:RFD000P2D27
```

Related Commands

license install
show license all
show license detail
show license expiring
show license feature
show license image-level
show license in-use
show license summary
license modify priority
show license evaluation

show 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.

Examples	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 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.

Examples This example shows how to display the current settings and buffer content details:

```
> show logging
Logging to buffer :
- Logging of system messages to buffer :
  - Logging filter level..... errors
  - Number of system messages logged..... 67227
  - Number of system messages dropped..... 21136
- Logging of debug messages to buffer ..... Disabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
Logging to console :
- Logging of system messages to console :
  - Logging filter level..... errors
  - Number of system messages logged..... 0
  - Number of system messages dropped..... 88363
- 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..... 67227
  - Number of system messages dropped..... 21136
- 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
  - Host 0..... Not Configured
  - Host 1..... Not Configured
  - Host 2..... Not Configured
Logging of traceback..... Disabled
Logging of process information..... Disabled
Logging of source file informational..... Enabled
Timestamping of messages.....
- Timestamping of system messages..... Enabled
  - Timestamp format..... Date and Time
- Timestamping of debug messages..... Enabled
  - Timestamp format..... Date and Time
Logging buffer (67227 logged, 21136 dropped)
*Apr 03 09:48:01.728: %MM-3-INVALID_PKT_RECVD: mm_listen.c:5508 Received an invalid
packet from 1.100.163.51. Source member:0.0.0.0. source member unknown.
*Apr 03 09:47:34.194: %LWAPP-3-DECODE_ERR: spam_lrad.c:1271 Error decoding discovery
request from AP 00:13:5f:0e:d4:20
*Apr 03 09:47:34.194: %LWAPP-3-DISC_OTAP_ERR: spam_lrad.c:5554 Ignoring OTAP discovery
request from AP 00:13:5f:0e:d4:20, OTAP is disabled
Previous message occurred 2 times.
```

Related Commands

config logging syslog host
config logging syslog facility
config logging syslog level

show login session

To display the existing sessions, use the **show login session** command.

show login session

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the current session details:

```
> show login session
ID      username      Connection From    Idle Time    Session Time
-----
00 admin          EIA-232           00:00:00      00:19:04
```

Related Commands **config login session 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.

Examples 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 **show netuser** command.

show netuser {**detail** *user_name* | **guest-roles** | **summary**}

Syntax Description

detail	Displays detailed information about the specified network user.
<i>user_name</i>	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.

Examples

This example shows how to display a summary of all users in the local user database:

```
> show netuser summary
Maximum logins allowed for a given username .....Unlimited
```

This example shows how to display detailed information on the specified network user:

```
> show netuser detail john10
username..... abc
WLAN Id..... Any
Lifetime..... Permanent
Description..... test user
```

Related Commands

config netuser add
config netuser delete
config netuser description
config netuser guest-role apply
config netuser wlan-id
config netuser guest-roles

show netuser guest-roles

To display a list of the current quality of service (QoS) roles and their bandwidth parameters, use the **show netuser guest-roles** command.

show netuser guest-roles

Syntax Description	This command has no arguments or keywords.

Command Default	None.

Examples	This example shows how to display a QoS role for the guest network user:

```
> show netuser guest-roles
Role Name..... Contractor
  Average Data Rate..... 10
  Burst Data Rate..... 10
  Average Realtime Rate..... 100
  Burst Realtime Rate..... 100
Role Name..... Vendor
  Average Data Rate..... unconfigured
  Burst Data Rate..... unconfigured
  Average Realtime Rate..... unconfigured
  Burst Realtime Rate..... unconfigured
```

Related Commands	config netuser add config netuser delete config netuser description config netuser guest-role apply config netuser wlan-id show netuser guest-roles show netuser

show network

To display the current status of 802.3 bridging for all WLANs, use the **show network** command.

show network

Syntax Description	This command has no arguments or keywords.

Command Default	None.

Examples	This example shows how to display the network details:

```
> 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.

Examples This example shows how to display a summary configuration:

```
> 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
oacp-600 dual-rlan-ports ..... Disable
oacp-600 local-network ..... Enable
mDNS snooping..... Disabled
```

mDNS Query Interval..... 15 minutes

Related Commands

config network

show network multicast mgid summary

show network multicast mgid detail

show network

show network multicast mgid detail

To display all the clients joined to the multicast group in a specific multicast group identification (MGID), use the **show network multicast mgid detail** command.

show network multicast mgid detail *mgid_value*

Syntax Description

<i>mgid_value</i>	Number between 550 and 4095.

Command Default

None.

Examples

This example shows how to display details of the multicast database:

```
> show network multicast mgid detail
Mgid ..... 550
Multicast Group Address ..... 239.255.255.250
Vlan ..... 0
Rx Packet Count ..... 807399588
No of clients ..... 1
Client List .....
  Client MAC      Expire Time (mm:ss)
    00:13:02:23:82:ad    0:20
```

Related Commands

show network summary
show network multicast mgid detail
show network

show network multicast mgid summary

To display all the multicast groups and their corresponding multicast group identifications (MGIDs), use the **show network multicast mgid summary** command.

show network multicast mgid summary

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display a summary of multicast groups and their MGIDs:

```
> show network multicast mgid summary
Layer2 MGID Mapping:
-----
InterfaceName          vlanId    MGID
-----
management              0         0
test                    0         9
wired                   20        8
Layer3 MGID Mapping:
-----
Number of Layer3 MGIDs ..... 1
Group address          Vlan      MGID
-----
239.255.255.250       0         550
```

Related Commands

- show network summary**
- show network multicast mgid detail**
- show network**

show nmsp notify-interval summary

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmsp notify-interval summary** command.

show nmsp notify-interval summary

Syntax Description	This command has no arguments or keywords.

Command Default	None.

Examples	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.

Examples

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
  Nmosp 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 Resp:     0
  Loc Subscr Req:    0      Loc Subscr Resp:  0
  Loc Notif:         0
  Loc Unsubscr Req:  0      Loc Unsubscr Resp: 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.

Examples

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.
<i>ip_addr</i>	Details only for the NMSP services subscribed to by a specific IP address.

Command Default

None.

Examples

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,
```

Related Commands

show nmsp notify-interval summary
show nmsp statistics
config nmsp notify-interval measurement
clear nmsp statistics
clear loop statistics

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.

Examples This example shows how to display NTP authentication key details:

```
> 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.

Examples

This example shows how to display QoS information for the silver profile:

```
> show qos
```

```
Description..... For Best Effort
Maximum Priority..... besteffort
Unicast Default Priority..... besteffort
Multicast Default Priority..... besteffort
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
protocol..... none
```

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.

Examples	This example shows how to display the scheduled system reset parameters:

```
> show reset
System reset is scheduled for Mar 27 01 :01 :01 2010
Current local time and date is Mar 24 02:57:44 2010
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel the reset.
Configuration will be saved before the system reset.
```

Related Commands	reset system at reset system in reset system cancel reset system notify-time

show route kernel

To display the kernel route cache information, use the **show route kernel** command.

show route kernel

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the kernel route cache information:

```
> show route kernel
Iface Destination Gateway Flags RefCnt Use Metric Mask MTU Window IRTT
dt10 14010100 00000000 0001 0 0 0 FFFFFFF0 0 0 0
dt10 28282800 00000000 0001 0 0 0 FFFFFFF0 0 0 0
dt10 34010100 00000000 0001 0 0 0 FFFFFFF0 0 0 0
eth0 02020200 00000000 0001 0 0 0 FFFFFFF0 0 0 0
dt10 33010100 00000000 0001 0 0 0 FFFFFFF0 0 0 0
dt10 0A010100 00000000 0001 0 0 0 FFFFFFF0 0 0 0
dt10 32010100 00000000 0001 0 0 0 FFFFFFF0 0 0 0
dt10 0A000000 0202020A 0003 0 0 0 FF000000 0 0 0
lo 7F000000 00000000 0001 0 0 0 FF000000 0 0 0
dt10 00000000 0A010109 0003 0 0 0 00000000 0 0 0
```

Related Commands

- clear ap
- debug arp
- show arp kernel
- config route add
- config route delete

show route summary

To display the routes assigned to the Cisco wireless LAN controller service port, use the **show route summary** command.

show route summary

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display all the configured routes:

```
> show route summary
Number of Routes..... 1
Destination Network      Genmask      Gateway
-----
xxx.xxx.xxx.xxx          255.255.255.0  xxx.xxx.xxx.xxx
```

Related Commands **config route**

show sessions

To display the console port login timeout and maximum number of simultaneous command-line interface (CLI) sessions, use the **show sessions** command.

show sessions

Syntax Description	This command has no arguments or keywords.

Command Default	5 minutes, 5 sessions.

Examples	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.

Examples 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.

Examples	This example shows how to display the SNMP engine ID:

```
> show snmpengineID
SNMP EngineId... ffffffff
```

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.

Examples 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
```

Related Commands

- config snmp trapreceiver create**
- config snmp trapreceiver delete**

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.

Examples 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.

Examples This example shows how to display the SNMP v1/v2/v3 status:

```
> show snmpversion
SNMP v1 Mode..... Disable
SNMP v2c Mode..... Enable
SNMP v3 Mode..... Enable
```

Related Commands **config snmp version**

show switchconfig

To display parameters that apply to the Cisco wireless LAN controller, use the **show switchconfig** command.

show switchconfig

Syntax Description	This command has no arguments or keywords.

Command Default	Enabled.

Examples	This example shows how to display parameters that apply to the Cisco wireless LAN controller:

```
> show switchconfig
802.3x Flow Control Mode..... Disabled
FIPS prerequisite features..... Enabled
Boot Break..... Enabled
secret obfuscation..... Enabled
Strong Password Check Features:
  case-check .....Disabled
  consecutive-check ....Disabled
  default-check .....Disabled
  username-check .....Disabled
```

Related Commands	config switchconfig mode
	config switchconfig secret-obfuscation
	config switchconfig strong-pwd
	config switchconfig flowcontrol
	config switchconfig fips-prerequisite
	show stats switch

show sysinfo

To display high-level Cisco wireless LAN controller information, use the **show sysinfo** command.

show sysinfo

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display wireless LAN controller information:

```
> show sysinfo
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 6.0.133.0
Build Information..... Tue Mar 31 11:44:12 PDT 2009
Bootloader Version..... 0.14.0
Field Recovery Image Version..... 5.3.38.0-BL-9-16
Firmware Version..... FPGA 1.0, Env 0.8, USB console 1.27
Build Type..... DATA + WPS
System Name..... 5500
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.9.1.1
IP Address..... 10.10.10.7
Last Reset..... Software reset
System Up Time..... 1 days 15 hrs 17 mins 48 secs
System Timezone Location.....
Current Boot License Level..... wplus
Current Boot License Type..... Permanent
Next Boot License Level..... wplus
Next Boot License Type..... Permanent
Configured Country..... US - United States
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +45 C
External Temperature..... +29 C
Fan Status..... OK
State of 802.11b Network..... Enabled
State of 802.11a Network..... Disabled
Number of WLANs..... 18
3rd Party Access Point Support..... Disabled
Number of Active Clients..... 1
Burned-in MAC Address..... 00:00:1B:EE:12:E0
Power Supply 1..... Not Available
Power Supply 2..... Not Available
Maximum number of APs supported..... 250
```

Related Commands **config sysname**

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.

Examples	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.

Examples 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.

Examples 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.

Examples This example shows how to display controller SNMP trap log settings:

```
> 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)
```

Related Commands **show trapflags**

Config Commands

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

Configure 802.11h Commands

Use the **config 802.11h** commands to configure settings specifically for an 802.11h network.

config 802.11h channelswitch

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

config 802.11h channelswitch {**enable** *mode value* | **disable**}

Syntax Description

enable	Enables the 802.11h channel switch announcement.
<i>mode</i>	802.11h channel switch announcement mode.
<i>value</i>	802.11h channel announcement value.
disable	Disables the 802.11h channel switch announcement.

Command Default

None.

Examples

This example shows how to disable the 802.11h switch announcement:

```
> config 802.11h channelswitch disable
```

Related Commands

show 802.11h

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

<i>value</i>	802.11h power constraint value.

Command Default

None.

Examples

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

```
> config 802.11h powerconstraint 5
```

Related Commands

show 802.11h

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

<i>cisco_ap</i>	Cisco lightweight access point name.

Command Default

None.

Examples

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

```
> config 802.11h setchannel ap02
```

Related Commands

show 802.11h

Configure 802.11 11n Support Commands

Use the **config 802.11 11n support** commands to configure settings for an 802.11n network.

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.

Examples

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

```
> config 802.11a 11nsupport enable
```

Related Commands

config 802.11 11nsupport mcs tx
config 802.11 11nsupport a-mpdu tx priority
config 802.11a disable network
config 802.11a disable
config 802.11a channel ap
config 802.11a txpower ap
config 802.11a chan_width

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

By 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.

Examples

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

```
> config 802.11a 11nsupport a-mpdu tx priority all enable
```

Related Commands

```
config 802.11 11nsupport mcs tx  
config 802.11a disable network  
config 802.11a disable  
config 802.11a channel ap  
config 802.11a txpower ap
```

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.
<i>timeout-value</i>	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.

Examples

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

```
> config 802.11 11nsupport a-mpdu tx scheduler timeout rt 100
```

Related Commands

config 802.11 11nsupport mcs tx
config 802.11a disable network
config 802.11a channel ap
config 802.11a txpower ap
config 802.11a chan_width

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.
<i>cisco_ap</i>	Access point.
A/B/C/D	Specifies an antenna port.
enable	Enables the configuration.
disable	Disables the configuration.

Command Default

None.

Examples

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

```
> config 802.11 11nsupport antenna AP1 C enable
```

Related Commands

config 802.11 11nsupport mcs tx
config 802.11a disable network
config 802.11a disable
config 802.11a channel ap
config 802.11a txpower ap
config 802.11a chan_width

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.

Examples

This example shows how to configure a long guard interval:

```
> config 802.11 11nsupport guard-interval long
```

Related Commands

config 802.11 11nsupport mcs tx
config 802.11a disable network
config 802.11a channel ap
config 802.11a txpower ap
config 802.11a chan_width

config 802.11 11n support 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 11n support mcs tx** command.

config 802.11 {a | b} 11n support mcs tx {0-15} {enable | disable}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
11n support	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.

Examples

This example shows how to specify MCS rates:

```
> config 802.11a 11nsupport mcs tx 5 enable
```

Related Commands

`config 802.11 11nsupport`
`config wlan wmm required`
`config 802.11 11nsupport a-mpdu tx priority`
`config 802.11a disable network`
`config 802.11a disable`
`config 802.11a channel ap`
`config 802.11a txpower ap`
`config 802.11a chan_width`

config 802.11 11n support rifs

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

config 802.11 {a | b} 11n support rifs {enable | disable}

Syntax Description

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

Command Default

None.

Examples

This example shows how to enable RIFS:

```
> config 802.11a 11n support rifs enable
```

Related Commands

config 802.11 11n support mcs tx
config 802.11a disable network
config 802.11a disable
config 802.11a channel ap
config 802.11a txpower ap
config 802.11a chan_width

Configure 802.11 CAC Commands

Use the **config 802.11 cac** commands to configure Call Admission Control (CAC) protocol settings.

config 802.11 cac defaults

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

config 802.11 {a | b} cac defaults

Syntax Description

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

Usage Guidelines

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

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

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

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

Examples

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

```
> 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

Disabled.

Usage Guidelines

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

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

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

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

Examples

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

```
> config 802.11 cac video acm enable
```

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

```
> config 802.11 cac video acm disable
```

Related Commands

config 802.11 cac video max-bandwidth
config 802.11 cac video roam-bandwidth
config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video cac-method

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

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

Syntax Description

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

Command Default

Static.

Usage Guidelines

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

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

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

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

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

Examples

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

```
> config 802.11 cac video cac-method static
```

Related Commands

```
show cac voice stats
show cac voice summary
show cac video stats
show cac video summary
config 802.11 cac video tspec-inactivity-timeout
config 802.11 cac video max-bandwidth
config 802.11 cac video acm
config 802.11 cac video sip
config 802.11 cac video roam-bandwidth
config 802.11 cac load-based
config 802.11 cac defaults
config 802.11 cac media-stream
config 802.11 cac multimedia
debug cac
```


config 802.11 cac video load-based

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

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

Syntax Description

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

Command Default

Disabled.

Usage Guidelines

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

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

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

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

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

**Note**

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

Examples

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

```
> 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.
<i>bandwidth</i>	Bandwidth percentage value from 5 to 85%.

Command Default

0%.

Usage Guidelines

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



Note

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

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

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

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

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

Examples

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

```
> 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.
<i>retry-percentage</i>	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.
<i>dot11-rate</i>	Minimum transmission data rate to the client for multicast-direct media streams. Rate in kbps at which the client can operate. If the transmission data rate is below this rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial. The available data rates are 6000, 9000, 12000, 18000, 24000, 36000, 48000, 54000, and 11n rates.

Command Default

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

Usage Guidelines

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

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

- Disable all WLANs with WMM enabled by entering the **config wlan disable wlan_id** command.
- Disable the radio network you want to configure by entering the **config 802.11 {a | b} disable network** command.
- Save the new configuration by entering the **save config** command.

- Enable voice or video CAC for the network you want to configure by entering the **config 802.11 {a | b} cac voice acm enable** or **config 802.11 {a | b} cac video acm enable** command.

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

Examples

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

```
> 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.
<i>bandwidth</i>	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 value is 85%.

Usage Guidelines

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

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

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

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

Examples

This 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:

```
> 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.
<i>bandwidth</i>	Bandwidth percentage value from 5 to 85%.

Command Default

0%.

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.

Examples

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

```
> 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 non-traffic specifications (TSPEC) SIP clients using video applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac video sip** command.

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

Syntax Description

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

Command Default

None.

Usage Guidelines

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

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

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

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

Examples

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

```
> 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

Disabled (ignore).

Usage Guidelines

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

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

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

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

Examples

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

```
> 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:

```
> 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

Disabled.

Usage Guidelines

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

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

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

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

Examples

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

```
> config 802.11c cac voice acm enable
```

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

```
> 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.
<i>bandwidth</i>	Bandwidth percentage value from 5 to 85%.

Command Default

0%.

Usage Guidelines

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

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

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

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

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

Examples

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

```
> 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.
<i>bandwidth</i>	Bandwidth percentage value from 0 to 85%.

Command Default

85%.

Usage Guidelines

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



Note

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

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

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

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

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

Examples

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

```
> config 802.11 cac voice roam-bandwidth 10
```

Related Commands

`config 802.11 cac voice acm`
`config 802.11 cac 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

Disabled (ignore).

Usage Guidelines

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

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

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

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

Examples

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

```
> 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 802.11 cac 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

Disabled.

Usage Guidelines

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

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

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

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

Examples

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

```
> config 802.11a cac voice load-based enable
```

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

```
> 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.
<i>number</i>	Number of calls to be allowed per radio.

Command Default

0, which means that there is no maximum limit check for the number of calls.

Usage Guidelines

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

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

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

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

Examples

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

```
> 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 in case of 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.
<i>bw_kbps</i>	Bandwidth in kbps.
sample-interval	Specifies the packetization interval for SIP codec.
<i>number_msecs</i>	Packetization sample interval in msecs. The sample interval for SIP codec is 20 seconds.

Command Default

None.

Usage Guidelines

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

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

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

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

Examples

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

```
> 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.
<i>number_msecs</i>	Packetization interval in msecs. The sample interval for SIP codec value is 20 seconds.

Command Default

g711.

Usage Guidelines

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

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

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

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

Examples

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

```
> 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:

```
> 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.
<i>stream_size</i>	Range of stream size is between 84000 and 92100.
<i>number</i>	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.
<i>mean_datarate</i>	Mean data rate (84 to 91.2 kbps) of a voice stream.

Command Default

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

Usage Guidelines

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

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

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

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

Examples

This 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:

```
> 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 Commands

Use the **config 802.11** commands to configure settings for an 802.11 network.

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.
<i>time_units</i>	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.

Examples

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

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

Command Default

The transmission is enabled for the entire network by default.

Usage Guidelines

Note

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.

Examples

This example shows how to disable the entire 802.11a network:

```
> config 802.11a disable network
```

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

```
> config 802.11b disable AP01
```

Related Commands

show sysinfo
show 802.11a
config 802.11a enable
config 802.11b disable
config 802.11b enable
config 802.11a beaconperiod

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

Enabled.

Examples

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

```
> config 802.11a dtpc disable
```

Related Commands

show 802.11a
config 802.11a beaconperiod
config 802.11a disable
config 802.11a enable

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

Command Default

The transmission is enabled for the entire network by default.

Usage Guidelines

Note

Use this command in conjunction 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.

Examples

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

```
> config 802.11a enable network
```

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

```
> config 802.11b enable AP1
```

Related Commands

show sysinfo show 802.11a

config wlan radio

config 802.11a disable

config 802.11b disable

config 802.11b enable

config 802.11b 11gSupport enable

config 802.11b 11gSupport disable

config 802.11 exp-bwreq

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

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

Syntax Description

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

Command Default

The expedited bandwidth request feature is disabled by default.

Usage Guidelines

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

Examples

This example shows how to enable the CCX expedited bandwidth settings:

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

This example shows how to disable the CCX expedited bandwidth settings:

```
> config 802.11a exp-bwreq disable
```

Related Commands

show 802.11a
show ap stats 802.11a

config 802.11 fragmentation

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

config 802.11 {a | b} fragmentation *threshold*

**Note**

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

Syntax Description

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

Command Default

None.

Examples

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

```
> config 802.11a fragmentation 6500
```

Related Commands

config 802.11b fragmentation
show 802.11b
show ap auto-rtf

config 802.11 l2roam rf-params

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
default	Restores Layer 2 client roaming RF parameters to default values.
custom	Configures custom Layer 2 client roaming RF parameters.
<i>min_rssi</i>	Minimum received signal strength indicator (RSSI) that is required for the client to associate to the access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. The valid range is –80 to –90 dBm, and the default value is –85 dBm.
<i>roam_hyst</i>	How much greater the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between the two access points. The valid range is 2 to 4 dB, and the default value is 2 dB.
<i>scan_thresh</i>	Minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold. The valid range is –70 to –77 dBm, and the default value is –72 dBm.
<i>trans_time</i>	Maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold. The valid range is 1 to 10 seconds, and the default value is 5 seconds.
Note For high-speed client roaming applications in outdoor mesh environments, we recommend that you set the transition time to 1 second.	

Command Default

<i>min_rssi</i>	-85
<i>roam_hyst</i>	2
<i>scan_thresh</i>	-72
<i>trans_time</i>	5

Usage Guidelines

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

Examples

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

```
> 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.
<i>max-clients</i>	Maximum number of client connections per access point. The range is from 1 to 200.

Command Default

None.

Examples

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

```
> 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 datarate, 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

<i>data_rate</i>	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.
<i>ap_name</i>	Specific AP radio in this datarate.
default	Configures all APs radio in this datarate.

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 datarate 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 datarate 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 APs already joined the controller. The APs that join the controller after the new datarate value is set will receive the new datarate value.

Examples

This example shows how to configure minimum multicast data rate settings:

```
> 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.
<i>rate</i>	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.

Examples

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

```
> config 802.11b rate mandatory 12
```

Related Commands

show ap config 802.11a

config 802.11b rate

config 802.11 tsm

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

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

Syntax Description

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

Command Default

Disabled.

Examples

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

```
> config 802.11b tsm enable
```

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

```
> config 802.11b tsm disable
```

Related Commands

show ap stats
show client tsm

Configure Advanced 802.11 Commands

Use the **config advanced 802.11** commands to configure advanced settings and devices on 802.11a, 802.11b/g, or other supported 802.11 networks.

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.
<i>limit</i>	Call admission limit (from 0 to 255). The default value is 105.
<i>quantum</i>	G711 quantum value. The default value is 15.

Command Default

None.

Examples

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

```
> 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 the 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}

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 when 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 when voice services other than Spectralink are deployed on your network.
optimized-video-voice	Enables EDCA voice- 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 (ACM) 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.

Command Default

wmm-default

Examples

This example shows how to enable Spectralink voice priority parameters:

```
> config advanced 802.11 edca-parameters svp-voice
```

Related Commands

show 802.11a
config advanced 802.11b edca-parameters

config advanced fastpath fastcache

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

config advanced fastpath fastcache {enable | disable}

Syntax Description

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

Command Default

None.

Examples

This example shows how to enable the fastpath fast cache control:

```
> config advanced fastpath fastcache enable
```

Related Commands

config advanced fastpath pkt-capture

config advanced fastpath pkt-capture

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

config advanced fastpath pkt-capture {enable | disable}

Syntax Description

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

Command Default

None.

Examples

This example shows how to enable the fastpath packet capture:

```
> config advanced fastpath pkt-capture enable
```

Related Commands

config advanced fastpath fastcache

config advanced sip-preferred-call-no

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

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

Syntax Description

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

Command Default

None.

Usage Guidelines

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

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

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

Examples

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

```
> config advanced sip-preferred-call-no 2 0123456789
```

Related Commands

```
config wlan qos
config 802.11 cac video acm
config 802.11 cac voice acm
config wlan call-snoop
show ap stats
```

config advanced sip-snooping-ports

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

config advanced sip-snooping-ports *start_port end_port*

Syntax Description

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

Usage Guidelines

If you need only a single port for call snooping, configure the start and end port with the same number. The port used by the CIUS tablet is 5060 and the port range used by Facetime is from 16384 to 16402.

Examples

This example shows how to configure the call snooping ports:

```
> config advanced sip-snooping-ports 4000 4500
```

Related Commands

show cac voice stats
show cac voice summary
show cac video stats
show cac video summary
config 802.11 cac video sip
config 802.11 cac voice sip
show advanced sip-preferred-call-no
show advanced sip-snooping-ports
debug cac

Configure AVC Commands

Use the **config avc** commands to configure Application and Visibility settings on the controller.

config avc profile create

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

config avc profile *profile_name* **create**

Syntax Description

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

Command Default

None.

Usage Guidelines

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

Examples

This example shows how to create a new AVC profile:

```
> config avc profile avcprofile1 create
```

Related Commands

config avc profile delete
config avc profile rule
config wlan avc
show avc profile
show avc applications
show avc statistics
debug avc error
debug avc events

config avc profile delete

To delete an AVC profile, use the **config avc profile delete** command.

config avc profile *profile_name* **delete**

Syntax Description

<i>profile_name</i>	Name of the AVC profile.
delete	Deletes an AVC profile.

Command Default

None.

Examples

This example shows how to delete an AVC profile:

```
> config avc profile avcprofile1 delete
```

Related Commands

config avc profile create
config avc profile rule
config wlan avc
show avc profile summary
show avc profile detailed
debug avc error
debug avc events

config avc profile rule

To configure a rule for an AVC profile, use the **config avc profile rule** command.

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

Syntax Description

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

Command Default

None.

Examples

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

```
> config avc profile avcprofile1 rule add application gmail mark 10
```

Related Commands

config avc profile delete
config avc profile create
config wlan avc
show avc profile
show avc applications
show avc statistics
debug avc error

debug avc events

config wlan avc

To configure Application Visibility and Control (AVC) on a WLAN, use the **config wlan avc** command.

config wlan avc *wlan_id* {**profile** *profile_name* | **visibility**} {**enable** | **disable**}

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
profile	Associates or removes an AVC profile from a WLAN.
<i>profile_name</i>	Name of the AVC profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
visibility	Configures application visibility on a WLAN.
enable	Enables application visibility on a WLAN. You can view the classification of applications based on the Network Based Application Recognition (NBAR) deep packet inspection technology. Use the show avc statistics client command to view the client AVC statistics.
disable	Disables application visibility on a WLAN.

Command Default

None.

Usage Guidelines

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

Examples

This example shows how to associate an AVC profile with a WLAN:

```
> config wlan avc 5 profile profile1 enable
```

Related Commands

config avc profile delete
config avc profile create
config avc profile rule
show avc statistics
show avc profile applications
show avc applications
show avc statistics client

show avc statistics wlan
show avc statistics top-apps
show avc statistics guest-lan
show avc statistics remote-lan
debug avc error
debug avc events

Configure Band-Select Commands

Use the **config band-select** command to configure the band selection feature on the controller.

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.

Examples

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

```
> 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.

Examples

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

```
> 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.
<i>seconds</i>	• Value for suppression between 10 to 200 seconds. • Value for a dual-band between 10 to 300 seconds.

Command Default

None.

Examples

This example shows how to set the suppression expire to 70 seconds:

```
> config band-select expire suppression 70
```

Related Commands

config band-select cycle-threshold
config band-select client-rssi
config band-select cycle-count

config band-select client-rssi

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

config band-select client-rssi *rssi*

Syntax Description

rssi

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

Command Default

None.

Examples

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

```
> config band-select client-rssi 70
```

Related Commands

config band-select cycle-threshold

config band-select expire

config band-select cycle-count

Configure Guest-LAN Commands

Use the **config guest-lan** commands to create, delete, enable, and disable the wireless LAN commands.

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:
<i>guest_lan_id</i>	LAN identifier between 1 and 5 (inclusive).
<i>interface_name</i>	Interface name up to 32 alphanumeric characters.
enable	Enables a wireless LAN.
disable	Disables a wireless LAN.

Command Default

None.

Examples

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

```
> 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 to specify the URL of the external server.

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

Syntax Description

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

Command Default

None.

Examples

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

```
> 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.

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.

Examples

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

```
> 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

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

Command Default

None.

Examples

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

```
> 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.
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Command Default

Internal.

Examples

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

```
> config guest-lan custom-web webauth-type internal 1
```

Related Commands

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

config guest-lan ingress-interface

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

config guest-lan ingress-interface *guest_lan_id interface_name*

Syntax Description

<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
<i>interface_name</i>	Interface name.

Command Default

None.

Examples

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

```
> config guest-lan ingress-interface 1 guest01
```

Related Commands

config interface guest-lan
config guest-lan create

config guest-lan interface

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

config guest-lan interface *guest_lan_id* *interface_name*

Syntax Description

<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
<i>interface_name</i>	Interface name.

Command Default

None.

Examples

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

```
> config guest-lan interface 1 guest01
```

Related Commands

config ingress-interface guest-lan
config guest-lan create

config guest-lan mobility anchor

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

config guest-lan mobility anchor {add | delete} *wlan_id* *anchor_ip*

Syntax Description

add	Adds a mobility anchor.
delete	Deletes a mobility anchor.
<i>wlan_id</i>	WLAN identifier.
<i>anchor_ip</i>	IP address of the mobility anchor.

Command Default

None.

Examples

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

```
> config guest-lan mobility anchor delete 4 192.168.0.14
```

Related Commands

config mobility group anchor
config mobility group domain
config mobility group keepalive count
config mobility group keepalive interval
config mobility group member
config mobility group multicast-address
config mobility multicast-mode
config mobility secure-mode
config wlan mobility anchor
debug mobility
show mobility anchor
show mobility statistics
show mobility summary

config guest-lan nac

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

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

Syntax Description

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

Command Default

None.

Examples

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

```
> config guest-lan nac enable 3
```

Related Commands

```
show nac statistics  
show nac summary  
config wlan nac  
debug nac
```

config guest-lan security

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

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

Syntax Description

web-auth	Specifies web authentication.
enable	Enables the web authentication settings.
disable	Disables the web authentication settings.
acl	Configures an access control list.
server-precedence	Configures the authentication server precedence order for web authentication users.
<i>guest_lan_id</i>	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

Web authentication.

Examples

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

```
> config guest-lan security web-auth enable 1
```

Related Commands

```
config ingress-interface guest-lan
config guest-lan create
config interface guest-lan
```

Configure mDNS Commands

Use the **config mdns** commands to configure Multicast DNS (mDNS) settings on the controller.

config interface group mdns-profile

To configure an mDNS profile for an interface group, use the **config interface group mdns-profile** command.

config interface group mdns-profile {all | *interface-group-name*} {*profile-name* | none}

Syntax Description

all	Configures an mDNS profile for all interface groups.
<i>interface-group-name</i>	Name of the interface group to which the mDNS profile has to be associated. The interface group name can be up to 32 case-sensitive, alphanumeric characters.
<i>profile-name</i>	Name of the mDNS profile.
none	Removes all existing mDNS profiles from the interface group. You cannot configure mDNS profiles on the interface group.

Command Default

None.

Usage Guidelines

If the mDNS profile is associated to a WLAN, an error appears.

Examples

This example shows how to configure an mDNS profile for an interface group floor1:

```
> config interface group mdns-profile floor1 profile1
```

Related Commands

config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config mdns profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns all
debug mdns error
debug mdns detail
debug mdns message

config interface mdns-profile

To configure an mDNS profile for an interface, use the **config interface mdns-profile** command.

config interface mdns-profile {**management** | **all** *interface-name*} {*profile-name* | **none**}

Syntax Description

management	Configures an mDNS profile for the management interface.
all	Configures an mDNS profile for all interfaces.
<i>interface-name</i>	Name of the interface on which the mDNS profile has to be configured. The interface name can be up to 32 case-sensitive, alphanumeric characters.
<i>profile-name</i>	Name of the mDNS profile.
none	Removes all existing mDNS profiles from the interface. You cannot configure mDNS profiles on the interface.

Command Default

None.

Usage Guidelines

If the mDNS profile is associated to a WLAN, an error appears.

Examples

This example shows how to configure an mDNS profile for an interface lab1:

```
> config interface mdns-profile lab1 profile1
```

Related Commands

config mdns query interval
config mdns service
config mdns snooping
config mdns profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns all
debug mdns error
debug mdns detail
debug mdns message

config mdns profile

To configure an mDNS profile and associate a service with the profile, use the **config mdns profile** command.

config mdns profile {create | delete | service {add | delete} *service _name* *profile _name*

Syntax Description

create	Creates an mDNS profile.
delete	Deletes an mDNS profile. If the profile is associated to an interface group, an interface, or a WLAN, an error appears.
service	Configures an mDNS service.
add	Adds an mDNS service to an mDNS profile.
delete	Deletes an mDNS service from an mDNS profile.
<i>service _name</i>	Name of the mDNS service.
<i>profile _name</i>	Name of the mDNS profile. You can create a maximum of 16 profiles.

Command Default

None.

Usage Guidelines

After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.

Examples

This example shows how to add the Apple TV mDNS service to the mDNS profile1:

```
> config mdns profile create profile1 Apple TV
```

Related Commands

config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config mdns query interval

To configure the query interval for mDNS services, use the **config mdns query interval** command.

config mdns query interval *interval_value*

Syntax Description

<i>interval_value</i>	mDNS query interval, in minutes that you can set. The query interval is the frequency at which the controller sends periodic queries to all the services defined in the Master Service database. The range is from 10 to 120 minutes.

Command Default

15 minutes.

Usage Guidelines

The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database. mDNS uses the multicast IP address 224.0.0.251 as the destination address and 5353 as UDP destination port.

Examples

This example shows how to configure the query interval for mDNS services as 20 minutes:

```
> config mdns query interval 20
```

Related Commands

- config mdns profile
- config mdns service
- config mdns snooping
- config interface mdns-profile
- config interface group mdns-profile
- config wlan mdns
- show mdns profile
- show mnds service
- clear mdns service-database
- debug mdns all
- debug mdns error
- debug mdns detail
- debug mdns message

config mdns service

To configure mDNS services in the Master Services database, use the **config mdns service** command.

config mdns service {**create** *service_name* *service_string* **query** {**enable** | **disable**} | **delete** *service_name* | **query** {**enable** | **disable**}}

Syntax Description

create	Adds a new mDNS service to the Master Services database.
<i>service_name</i>	Name of the mDNS service. For example, Air Tunes, iTunes Music Sharing, FTP, Apple File Sharing Protocol (AFP).
<i>service_string</i>	Unique string associated to an mDNS service. For example, “_airplay._tcp.local.” is the service string associated with Apple TV.
query	Configures the query status for the mDNS service.
enable	Enables periodic query for an mDNS service by the controller.
disable	Disables periodic query for an mDNS service by the controller.
delete	Deletes an mDNS service from the Master Services database. Before deleting the service, the controller checks if any profile uses the service. You must delete the service from all profiles before deleting the service.

Command Default

None.

Usage Guidelines

The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database. The controller can snoop and learn a maximum of 64 services.

Examples

This example shows how to add the Apple TV mDNS service to the Master Services database:

```
> config mdns service create Apple TV _airplay._tcp.local. query enable
```

Related Commands

config mdns query interval
config mdns profile
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config mdns snooping

To enable or disable global mDNS snooping on the controller, use the **config mdns snooping** command.

config mdns snooping {enable | disable}

Syntax Description

enable	Enables mDNS snooping on the controller.
disable	Disables mDNS snooping on the controller.

Command Default

Enabled.

Usage Guidelines

Multicast DNS (mDNS) service discovery provides a way to announce and discover services on the local network. mDNS perform DNS queries over IP multicast. mDNS supports zero configuration IP networking.

Examples

This example shows how to enable mDNS snooping:

```
> config mdns snooping enable
```

Related Commands

config mdns query interval
config mdns service
config mdns profile
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns all
debug mdns error
debug mdns detail
debug mdns message

config wlan mdns

To configure an multicast DNS (mDNS) profile for a WLAN, use the **config wlan mdns** command.

config wlan mdns {**enable** | **disable** | **profile** {*profile-name* | **none**}} {*wlan_id* | **all**}

Syntax Description

enable	Enables mDNS snooping on a WLAN.
disable	Disables mDNS snooping on a WLAN.
profile	Configures an mDNS profile for a WLAN.
<i>profile-name</i>	Name of the mDNS profile to be associated with a WLAN.
none	Removes all existing mDNS profiles from the WLAN. You cannot configure mDNS profiles on the WLAN.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
all	Configures the mDNS profile for all WLANs.

Command Default

Enabled.

Usage Guidelines

You must disable the WLAN before you use this command. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

Examples

This example shows how to configure an mDNS profile for a WLAN:

```
> config wlan mdns profile profile1 1
```

Related Commands

config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config mdns profile
show mdns profile
show mnds service
clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

Configure Management-User Commands

Use the **config mgmtuser** commands to configure management user settings.

config mgmtuser add

To add a local management user to the Cisco wireless LAN controller, use the **config mgmtuser add** command.

config mgmtuser add *username password* {**read-write** | **read-only**} [*description*]

Syntax Description

<i>username</i>	Account username. The username can be up to 24 alphanumeric characters.
<i>password</i>	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.
<i>description</i>	(Optional) Description of the account. The description can be up to 32 alphanumeric characters within double quotes.

Command Default

None.

Examples

This example shows how to create a management user account with read-write access:

```
> config mgmtuser add admin admin read-write "Main account"
```

Related Commands

show mgmtuser

config mgmtuser delete

To delete a management user from the Cisco wireless LAN controller, use the **config mgmtuser delete** command.

config mgmtuser delete *username*

Syntax Description

<i>username</i>	Account username. The username can be up to 24 alphanumeric characters.

Command Default

None.

Examples

This example shows how to delete a management user account admin from the Cisco wireless LAN 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 Cisco wireless LAN controller, use the **config mgmtuser description** command.

config mgmtuser description *username description*

Syntax Description

<i>username</i>	Account username. The username can be up to 24 alphanumeric characters.
<i>description</i>	Description of the account. The description can be up to 32 alphanumeric characters within double quotes.

Command Default

None.

Examples

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

```
> config mgmtuser description admin "master user"
```

Related Commands

config mgmtuser add
config mgmtuser delete
config mgmtuser password
show mgmtuser

config mgmtuser password

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

config mgmtuser password *username password*

Syntax Description

<i>username</i>	Account username. The username can be up to 24 alphanumeric characters.
<i>password</i>	Account password. The password can be up to 24 alphanumeric characters.

Command Default

None.

Examples

This example shows how to change the password of the management user “admin” with the new password 5rTfm:

```
> config mgmtuser password admin 5rTfm
```

Related Commands

show mgmtuser

Configure Net User Commands

Use the **config netuser** commands to configure netuser settings.

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

<i>username</i>	Guest username. The username can be up to 50 alphanumeric characters.
<i>password</i>	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.
<i>wlan_id</i>	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.
<i>guestlan_id</i>	Guest LAN ID.
userType	Specifies the user type.
guest	Specifies the guest for the guest user.
lifetime	Specifies the lifetime.
<i>lifetime</i>	Lifetime value (60 to 259200 or 0) in seconds for the guest user. Note A value of 0 indicates an unlimited lifetime.
<i>description</i>	Short description of user. The description can be up to 32 characters enclosed in double-quotes.

Command Default

None.

Usage Guidelines

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

Examples

This example shows how to add a permanent username Jane to the wireless network for 1 hour:

```
> config netuser add jane able2 1 wlan_id 1 userType permanent
```

This example shows how to add a guest username George to the wireless network for 1 hour:

```
> config netuser add george able1 guestlan 1 3600
```

Related Commands`show netuser``config netuser delete`

config netuser delete

To delete an existing user from the local network, use the **config netuser delete** command.

config netuser delete *username*

Syntax Description

<i>username</i>	Network username. The username can be up to 24 alphanumeric characters.

Command Default

None.

Usage Guidelines

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

Examples

This example shows how to delete an existing username named able1 from the network:

```
> 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

<i>username</i>	Network username. The username can contain up to 24 alphanumeric characters.
<i>description</i>	(Optional) User description. The description can be up to 32 alphanumeric characters enclosed in double quotes.

Command Default

None.

Examples

This example shows how to add a user description “HQ1 Contact” to an existing network user named able 1:

```
> 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

<i>username</i>	Network username. The username can be 24 alphanumeric characters.
<i>lan_id</i>	Wired guest LAN identifier to associate with the user. A zero value associates the user with any wired LAN.

Command Default

None.

Examples

This example shows how to configure a wired LAN ID 2 to associate with the user named aire1:

```
> config netuser guest-lan-id aire1 2
```

Related Commands

show netuser
show wlan summary

config netuser guest-role apply

To apply a quality of service (QoS) role to a guest user, use the **config netuser guest-role apply** command.

config netuser guest-role apply *username* *role_name*

Syntax Description

<i>username</i>	Name of the user.
<i>role_name</i>	QoS guest role name.

Command Default

None.

Usage Guidelines

If you do not assign a QoS role to a guest user, the Role field in the User Details shows the role as default. The bandwidth contracts for this user are defined in the QoS profile for the WLAN.

If you want to unassign a QoS role from a guest user, use the **config netuser guest-role apply** *username* **default**. This user now uses the bandwidth contracts defined in the QoS profile for the WLAN.

Examples

This example shows how to apply a QoS role to a guest user jsmith with the QoS guest role named Contractor:

```
> config netuser guest-role apply jsmith Contractor
```

Related Commands

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role create

To create a quality of service (QoS) role for a guest user, use the **config netuser guest-role create** command.

config netuser guest-role create *role_name*

Syntax Description

<i>role name</i>	QoS guest role name.

Command Default

None.

Usage Guidelines

To delete a QoS role, use the **config netuser guest-role delete** role-name.

Examples

This example shows how to create a QoS role for the guest user named guestuser1:

```
> config netuser guest-role create guestuser1
```

Related Commands

config netuser guest-role delete

config netuser guest-role delete

To delete a quality of service (QoS) role for a guest user, use the **config netuser guest-role delete** command.

config netuser guest-role delete *role_name*

Syntax Description

<i>role_name</i>	Quality of service (QoS) guest role name.

Command Default

None.

Examples

This example shows how to delete a quality of service (QoS) role for guestuser1:

```
> config netuser guest-role delete guestuser1
```

Related Commands

config netuser guest-role create

config netuser guest-role qos data-rate average-data-rate

To configure the average data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate average-data-rate** command.

config netuser guest-role qos data-rate average-data-rate *role_name* *rate*

Syntax Description

<i>role_name</i>	Quality of service (QoS) guest role name.
<i>rate</i>	Rate for TCP traffic on a per user basis.

Command Default

None.

Usage Guidelines

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Examples

This example shows how to configure an average rate for the QoS guest named guestuser1:

```
> config netuser guest-role qos data-rate average-data-rate guestuser1 0
```

Related Commands

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role qos data-rate burst-data-rate

config netuser guest-role qos data-rate average-realtime-rate

To configure the average data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate average-realtime-rate** command.

config netuser guest-role qos data-rate average-realtime-rate *role_name* *rate*

Syntax Description

<i>role_name</i>	Quality of service (QoS) guest role name.
<i>rate</i>	Rate for TCP traffic on a per user basis.

Command Default

None.

Usage Guidelines

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Examples

This example shows how to configure an average data rate for the QoS guest user named guestuser1 with the rate for TCP traffic of 0 Kbps:

```
> config netuser guest-role qos data-rate average-realtime-rate guestuser1 0
```

Related Commands

config netuser guest-role

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-data-rate

To configure the peak data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate burst-data-rate** command.

config netuser guest-role qos data-rate burst-data-rate *role_name* *rate*

Syntax Description

<i>role_name</i>	Quality of service (QoS) guest role name.
<i>rate</i>	Rate for TCP traffic on a per user basis.

Command Default

None.

Usage Guidelines

The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Examples

This example shows how to configure the peak data rate for the QoS guest named guestuser1 with the rate for TCP traffic of 0 Kbps:

```
> config netuser guest-role qos data-rate burst-data-rate guestuser1 0
```

Related Commands

config netuser guest-role create
config netuser guest-role delete
config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-realtime-rate

To configure the burst real-time data rate for UDP traffic on a per user basis, use the **config netuser guest-role qos data-rate burst-realtime-rate** command.

config netuser guest-role qos data-rate burst-realtime-rate *role_name* *rate*

Syntax Description

<i>role_name</i>	Quality of service (QoS) guest role name.
<i>rate</i>	Rate for TCP traffic on a per user basis.

Command Default

None.

Usage Guidelines

The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the quality of service (QoS) policy may block traffic to and from the wireless client.

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Examples

This example shows how to configure a burst real-time rate for the QoS guest user named guestuser1 with the rate for TCP traffic of 0 Kbps:

```
> config netuser guest-role qos data-rate burst-realtime-rate guestuser1 0
```

Related Commands

config netuser guest-role

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-data-rate

config netuser lifetime

To configure the lifetime for a guest network user, use the **config netuser lifetime** command.

config netuser lifetime *username time*

Syntax Description

<i>username</i>	Network username. The username can be up to 50 alphanumeric characters.
<i>time</i>	Lifetime between 60 to 2592000 seconds or 0 for no limit.

Command Default

None.

Examples

This example shows how to configure a the lifetime for a guest network user:

```
> 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

0 (unlimited)

Examples

This example shows how to configure the maximum number of login sessions for a single user to 8:

```
> 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

<i>username</i>	Network username. The username can be up to 24 alphanumeric characters.
<i>password</i>	Network user password. The password can contain up to 24 alphanumeric characters.

Command Default

None.

Examples

This example shows how to change the network user password from aire1 to aire2:

```
> 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

<i>username</i>	Network username. The username can be 24 alphanumeric characters.
<i>wlan_id</i>	Wireless LAN identifier to associate with the user. A zero value associates the user with any wireless LAN.

Command Default

None.

Examples

This example shows how to configure a wireless LAN ID 2 to associate with the user named aire1:

```
> config netuser wlan-id aire1 2
```

Related Commands

show netuser

show wlan summary

Configure Network Commands

Use the **config network** commands to configure network settings.

config network 802.3-bridging

To enable or disable 802.3 bridging on a controller, use the **config network 802.3-bridging** command.

config network 802.3-bridging {enable | disable}

Syntax Description

enable	Enables the 802.3 bridging.
disable	Disables the 802.3 bridging.

Command Default

Disabled.

Usage Guidelines

In controller software release 5.2, the software-based forwarding architecture for Cisco 2100 Series Controllers is being replaced with a new forwarding plane architecture. As a result, Cisco 2100 Series Controllers and the Cisco wireless LAN controller Network Module for Cisco Integrated Services Routers bridge 802.3 packets by default. Therefore, 802.3 bridging can now be disabled only on Cisco 4400 Series Controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch.

To determine the status of 802.3 bridging, enter the **show netuser guest-roles** command.

Examples

This example shows how to enable the 802.3 bridging:

```
> config network 802.3-bridging enable
```

Related Commands

show netuser guest-roles
show network

config network allow-old-bridge-aps

To configure an old bridge access point's ability to associate with a switch, use the **config network allow-old-bridge-aps** command.

config network allow-old-bridge-aps {enable | disable}

Syntax Description

enable	Enables the switch association.
disable	Disables the switch association.

Command Default

Enabled.

Examples

This example shows how to configure an old bridge access point to associate with the switch:

```
> config network allow-old-bridge-aps enable
```

Related Commands

show network summary

config network ap-discovery

To enable or disable NAT IP in an AP discovery response, use the **config network ap-discovery** command.

config network ap-discovery nat-ip-only {enable | disable}

Syntax Description

enable	Enables use of NAT IP only in discovery response. This is the default.
disable	Enables use of both NAT IP and non NAT IP in discovery response.

Command Default

Enabled.

Usage Guidelines

If the **config interface nat-address management** command is set, this command controls which address(es) are sent in the CAPWAP discovery responses.

If all APs are on the outside of the NAT gateway of the controller, enter the **config network ap-discovery nat-ip-only enable** command, and only the management NAT address is sent.

If the controller has both APs on the outside and the inside of its NAT gateway, enter the **config network ap-discovery nat-ip-only disable** command, and both the management NAT address and the management inside address are sent. Ensure that you have entered the **config ap link-latency disable all** command to avoid stranding APs.

Examples

This example shows how to enable NAT IP in an AP discovery response:

```
> config network ap-discovery nat-ip-only enable
```

config network ap-fallback

To configure Cisco lightweight access point fallback, use the **config network ap-fallback** command.

config network ap-fallback {enable | disable}

Syntax Description

enable	Enables the Cisco lightweight access point fallback.
disable	Disables the Cisco lightweight access point fallback.

Command Default

Enabled.

Examples

This example shows how to enable the Cisco lightweight access point fallback:

```
> config network ap-fallback enable
```

Related Commands

show network summary

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

Disabled.

Examples

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

```
> config network ap-priority enable
```

Related Commands

config ap priority
show ap summary
show network summary

config network apple-talk

To configure AppleTalk bridging, use the **config network apple-talk** command.

config network apple-talk {enable | disable}

Syntax Description

enable	Enables the AppleTalk bridging.
disable	Disables the AppleTalk bridging.

Command Default

None.

Examples

This example shows how to configure AppleTalk bridging:

```
> config network apple-talk enable
```

Related Commands

show network summary

config network arptimeout

To set the Address Resolution Protocol (ARP) entry timeout value, use the **config network arptimeout** command.

config network arptimeout *seconds*

Syntax Description

seconds

Timeout in seconds. The minimum value is 10. The default value is 300.

Command Default

300.

Examples

This example shows how to set the ARP entry timeout value to 240 seconds:

```
> config network arptimeout 240
```

Related Commands

show network summary

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

config network bridging-shared-secret *shared_secret*

Syntax Description

<i>shared_secret</i>	Bridging shared secret string. The string can contain up to 10 bytes.

Command Default

Enabled.

Usage Guidelines

This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.

The zero-touch configuration must be enabled for this command to work.

Examples

This example shows how to configure the bridging shared secret string “shhh1”:

```
> config network bridging-shared-secret shhh1
```

Related Commands

show network summary

config network broadcast

To enable or disable broadcast packet forwarding, use the **config network broadcast** command.

config network broadcast {enable | disable}

Syntax Description

enable	Enables the broadcast packet forwarding.
disable	Disables the broadcast packet forwarding.

Command Default

Disabled.

Usage Guidelines

This command allows you to enable or disable broadcasting. You must enable multicast mode before enabling broadcast forwarding. Use the **config network multicast mode command** to configure multicast mode on the controller.



Note

The default multicast mode is unicast in case of all controllers except for Cisco 2106 Controllers. The broadcast packets and multicast packets can be independently controlled. If multicast is off and broadcast is on, broadcast packets still reach the access points, based on the configured multicast mode.

Examples

This example shows how to enable broadcast packet forwarding:

```
> 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.

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.

Examples

This example shows how to enable the fast SSID changing for mobile stations:

```
> config network fast-ssid-change enable
```

Related Commands

show network summary

config network ip-mac-binding

To validate the source IP address and MAC address binding within client packets, use the **config network ip-mac-binding** command.

config network ip-network-binding {enable | disable}

Syntax Description

enable	Enables this command.
disable	Disables this command.

Command Default

Enabled.

Usage Guidelines

In controller software release 5.2, the controller enforces strict IP address-to-MAC address binding in client packets. The controller checks the IP address and MAC address in a packet, compares them to the addresses that are registered with the controller, and forwards the packet only if they both match. In previous releases, the controller checks only the MAC address of the client and ignores the IP address.



Note

You might want to disable this binding check if you have a routed network behind a workgroup bridge (WGB).

Examples

This example shows how to validate the source IP and MAC address within client packets:

```
> config network ip-mac-binding enable
```

config network master-base

To enable or disable the Cisco wireless LAN controller as an access point default master, use the **config network master-base** command.

config network master-base {enable | disable}

Syntax Description

enable	Enables the Cisco wireless LAN controller acting as a Cisco lightweight access point default master.
disable	Disables the Cisco wireless LAN controller acting as a Cisco lightweight access point default master.

Command Default

None.

Usage Guidelines

This setting is only used upon network installation and should be disabled after the initial network configuration. Because the Master Cisco wireless LAN controller is normally not used in a deployed network, the Master Cisco wireless LAN controller setting can be saved from 6.0.199.0 or later releases.

Examples

This example shows how to enable the Cisco wireless LAN controller as a default master:

```
> config network master-base enable
```

config network mgmt-via-wireless

To enable Cisco wireless LAN controller management from an associated wireless client, use the **config network mgmt-via-wireless** command.

config network mgmt-via-wireless {enable | disable}

Syntax Description

enable	Enables the switch management from a wireless interface.
disable	Disables the switch management from a wireless interface.

Command Default

Disabled.

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.

Examples

This example shows how to configure switch management from a wireless interface:

```
> 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

Disabled.

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.

Examples

This example shows how to enable the global multicast support:

```
> 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

<i>value</i>	Frequency at which controller sends IGMP query messages. The range is from 15 to 2400 seconds.

Command Default

20 seconds.

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.

Examples

This example shows how to configure the IGMP query interval at 20 seconds:

```
> 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.

Examples

This example shows how to enable internet IGMP snooping settings:

```
> 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

<i>value</i>	Timeout range from 30 to 7200 seconds.

Command Default

None.

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.

Examples

This example shows how to configure the timeout value 50 for IGMP network settings:

```
> 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.
<i>interface-name</i>	Interface name for which the Layer 2 multicast is to enabled or disabled.

Command Default

None.

Examples

This example shows how to enable Layer 2 multicast for all interfaces:

```
> config network multicast l2mcast enable all
```

Related Commands

config network multicast global
config network multicast igmp snooping
config network multicast igmp query interval
config network multicast mld

config network multicast mld

To configure the Multicast Listener Discovery (MLD) parameters, use the **config network multicast mld** command.

config network multicast mld {**query interval** *interval-value* | **snooping** {**enable** | **disable**} | **timeout** *timeout-value*}

Syntax Description

query interval	Configures query interval to send MLD query messages.
<i>interval-value</i>	Query interval in seconds. The range is from 15 to 2400 seconds.
snooping	Configures MLD snooping.
enable	Enables MLD snooping.
disable	Disables MLD snooping.
timeout	Configures MLD timeout.
<i>timeout-value</i>	Timeout value in seconds. The range is from 30 seconds to 7200 seconds.

Command Default

None.

Examples

This example shows how to set a query interval of 20 seconds for MLD query messages:

```
> config network multicast mld query interval 20
```

Related Commands

config network multicast global
config network multicast igmp snooping
config network multicast igmp query interval
config network multicast l2mcast

config network multicast mode multicast

To configure the controller to use the multicast method to send broadcast or multicast packets to an access point, use the **config network multicast mode multicast** command.

config network multicast mode multicast

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to configure the multicast mode to send a single copy of data to multiple receivers:

```
> 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.

Examples This example shows how to configure the controller to use the unicast mode:

```
> config network multicast mode unicast
```

Related Commands

- config network multicast global**
- config network broadcast**
- config network multicast mode multicast**

config network oeap-600 dual-rlan-ports

To configure the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4, use the **config network oeap-600 dual-rlan-ports** command.

config network oeap-600 dual-rlan-ports {enable | disable}

Syntax Description

enable	Enables Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4.
disable	Resets the Ethernet port 3 Cisco OfficeExtend 600 Series access points to function as a local LAN port.

Command Default

Disabled.

Examples

This example shows how to enable the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port:

```
> config network oeap-600 dual-rlan-ports enable
```

Related Commands

show network summary

config network oeap-600 local-network

To configure access to the local network for the Cisco 600 Series OfficeExtend access points, use the **config network oeap-600 local-network** command.

config network oeap-600 local-network {enable | disable}

Syntax Description

enable	Enables access to the local network for the Cisco 600 Series OfficeExtend access points.
disable	Disables access to the local network for the Cisco 600 Series OfficeExtend access points.

Command Default

Disabled.

Examples

This example shows how to enable access to the local network for the Cisco 600 Series OfficeExtend access points:

```
> config network oeap-600 local-network enable
```

Related Commands

show network summary

config network otap-mode

To enable or disable over-the-air provisioning (OTAP) of Cisco lightweight access points, use the **config network otap-mode** command.

config network otap-mode {enable | disable}

Syntax Description

enable	Enables the OTAP provisioning.
disable	Disables the OTAP provisioning.

Command Default

Enabled.

Examples

This example shows how to disable the OTAP provisioning:

```
> config network otap-mode disable
```

Related Commands

show network summary

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

<i>name</i>	RF-Network name. The name can contain up to 19 characters.

Command Default

None.

Examples

This example shows how to set the RF-network name to travelers:

```
> config network rf-network-name travelers
```

Related Commands

show network summary

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

Enabled.

Usage Guidelines

This command allows management users to access the controller GUI using an http://ip-address. Web mode is not a secure connection.

Examples

This example shows how to enable the secure web interface settings for management users:

```
> 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 disabled for secure web mode with increased security and **enabled** for SSL v2.

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.

Examples

This example shows how to enable secure web mode with increased security:

```
> config network secureweb cipher-option
```

This example shows how to disable SSL v2:

```
> config network secureweb cipher-option sslv2 disable
```

Related Commands

config network secureweb
show network summary

config network ssh

To allow or disallow new Secure Shell (SSH) sessions, use the **config network ssh** command.

config network ssh {enable | disable}

Syntax Description

enable	Allows the new SSH sessions.
disable	Disallows the new SSH sessions.

Command Default

Disabled.

Examples

This example shows how to enable the new SSH session:

```
> config network ssh enable
```

Related Commands

show network summary

config network telnet

To allow or disallow new Telnet sessions, use the **config network telnet** command.

config network telnet {enable | disable}

Syntax Description

enable	Allows new Telnet sessions.
disable	Disallows new Telnet sessions.

Command Default

Disabled.

Examples

This example shows how to configure the new Telnet sessions:

```
> 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	<i>seconds</i>	Timeout duration in seconds. The minimum value is 90. The default value is 300.
Command Default	300.	
Usage Guidelines	Use this command to set the idle client session duration on the Cisco wireless LAN controller. The minimum duration is 90 seconds.	
Examples	This example shows how to configure the idle session timeout to 1200 seconds: > 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.

Examples

This example shows how to configure the controller to support bypass of captive portals:

```
> config network web-auth captive-bypass enable
```

Related Commands

show network summary
config network web-auth cmcc-support

config network web-auth cmcc-support

To configure eWalk on the controller, use the **config network web-auth cmcc-support** command.

config network web-auth cmcc-support {enable | disable}

Syntax Description

enable	Enables eWalk on the controller.
disable	Disables eWalk on the controller.

Command Default

None.

Examples

This example shows how to enable eWalk on the controller:

```
> config network web-auth cmcc-support enable
```

Related Commands

show network summary
config network web-auth captive-bypass

config network web-auth port

To configure an additional port to be redirected for web authentication at the network level, use the **config network web-auth port** command.

config network web-auth port *port*

Syntax Description

<i>port</i>	Port number. The valid range is from 0 to 65535.

Command Default

None.

Examples

This example shows how to configure an additional port number 1200 to be redirected for web authentication:

```
> config network web-auth port 1200
```

Related Commands

show network summary

config network web-auth proxy-redirect

To configure proxy redirect support for web authentication clients, use the **config network web-auth proxy-redirect** command.

config network web-auth proxy-redirect {enable | disable}

Syntax Description

enable	Allows proxy redirect support for web authentication clients.
disable	Disallows proxy redirect support for web authentication clients.

Command Default

None.

Examples

This example shows how to enable proxy redirect support for web authentication clients:

```
> config network web-auth proxy-redirect enable
```

Related Commands

show network summary

config network web-auth secureweb

To configure the secure web (https) authentication for clients, use the **config network web-auth secureweb** command.

config network web-auth secureweb {enable | disable}

Syntax Description

enable	Allows secure web (https) authentication for clients.
disable	Disallows secure web (https) authentication for clients. Enables http for Web Auth clients.

Command Default

Enabled.

Examples

This example shows how to enable the secure web (https) authentication for clients:

```
> 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

Enabled.

Examples

This example shows how to disable the web interface mode:

```
> 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.
<i>port-number</i>	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

Disabled.

Usage Guidelines

You must reset the system for the configuration to take effect.

Examples

This example shows how to enable proxy redirect support for web authentication clients:

```
> config network web-auth proxy-redirect enable
```

Related Commands

show network summary
show run-config
config qos protocol-type

config network zero-config

To configure bridge access point ZeroConfig support, use the **config network zero-config** command.

config network zero-config {enable | disable}

Syntax Description

enable	Enables the bridge access point ZeroConfig support.
disable	Disables the bridge access point ZeroConfig support.

Command Default

Enabled.

Examples

This example shows how to enable the bridge access point ZeroConfig support:

```
> config network zero-config enable
```

Related Commands

show network summary

Configure QoS Commands

Use the **config qos** commands to configure Quality of Service (QoS) settings.

config qos average-data-rate

To define the average data rate in Kbps for TCP traffic per user or per service set identifier (SSID), use the **config qos average-data-rate** command.

config qos average-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Syntax Description

bronze	Specifies the average data rate for the queue bronze.
silver	Specifies the average data rate for the queue silver.
gold	Specifies the average data rate for the queue gold.
platinum	Specifies the average data rate for the queue platinum.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
<i>rate</i>	Average data rate for TCP traffic per user. A value between 0 and 51,200 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None.

Examples

This example shows how to configure the average data rate 0 Kbps for the queue gold per SSID:

```
> config qos average-data-rate gold per ssid downstream 0
```

Related Commands

config qos burst-data-rate
config qos average-realtime-rate
config qos burst-realtime-rate
config wlan override-rate-limit

config qos average-realtime-rate

To define the average real-time data rate in Kbps for UDP traffic per user or per service set identifier (SSID), use the **config qos average-realtime-rate** command.

config qos average-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Syntax Description

bronze	Specifies the average real-time data rate for the queue bronze.
silver	Specifies the average real-time data rate for the queue silver.
gold	Specifies the average real-time data rate for the queue gold.
platinum	Specifies the average real-time data rate for the queue platinum.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
<i>rate</i>	Average real-time data rate for UDP traffic per user. A value between 0 and 51,200 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None.

Examples

This example shows how to configure the average real-time actual rate for queue gold:

```
> config qos average-realtime-rate gold per ssid downstream 10
```

Related Commands

config qos average-data-rate
config qos burst-data-rate
config qos burst-realtime-rate
config wlan override-rate-limit

config qos burst-data-rate

To define the peak data rate in Kbps for TCP traffic per user or per service set identifier (SSID), use the **config qos burst-data-rate** command.

config qos burst-data-rate {bronze | silver | gold | platinum} {per-ssid | per-client} {downstream | upstream} *rate*

Syntax Description

bronze	Specifies the peak data rate for the queue bronze.
silver	Specifies the peak data rate for the queue silver.
gold	Specifies the peak data rate for the queue gold.
platinum	Specifies the peak data rate for the queue platinum.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
<i>rate</i>	Peak data rate for TCP traffic per user. A value between 0 and 51,200 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None.

Examples

This example shows how to configure the peak rate 30000 Kbps for the queue gold:

```
> config qos burst-data-rate gold per ssid downstream 30000
```

Related Commands

config qos average-data-rate
config qos average-realtime-rate
config qos burst-realtime-rate
config wlan override-rate-limit

config qos burst-realtime-rate

To define the burst real-time data rate in Kbps for UDP traffic per user or per service set identifier (SSID), use the **config qos burst-realtime-rate** command.

config qos burst-realtime-rate {bronze | silver | gold | platinum} { per-ssid | per-client } { downstream | upstream } *rate*

Syntax Description

bronze	Specifies the burst real-time data rate for the queue bronze.
silver	Specifies the burst real-time data rate for the queue silver.
gold	Specifies the burst real-time data rate for the queue gold.
platinum	Specifies the burst real-time data rate for the queue platinum.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
<i>rate</i>	Burst real-time data rate for UDP traffic per user. A value between 0 and 51,200 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None.

Examples

This example shows how to configure the burst real-time actual rate 2000 Kbps for the queue gold:

```
> config qos burst-realtime-rate gold per ssid downstream 2000
```

Related Commands

config qos average-data-rate
config qos burst-data-rate
config qos average-realtime-rate
config wlan override-rate-limit

config qos description

To change the profile description, use the **config qos description** command.

config qos description {**bronze** | **silver** | **gold** | **platinum**} *description*

Syntax Description

bronze	Specifies the QoS profile description for the queue bronze.
silver	Specifies the QoS profile description for the queue silver.
gold	Specifies the QoS profile description for the queue gold.
platinum	Specifies the QoS profile description for the queue platinum.
<i>description</i>	QoS profile description.

Command Default

None.

Examples

This example shows how to configure the QoS profile description “description” for the queue gold:

```
> 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.
<i>usage-percentage</i>	Maximum percentage of RF usage.

Command Default

None.

Examples

This example shows how to specify the maximum percentage of RF usage for the queue gold:

```
> config qos max-rf-usage gold 20
```

Related Commands

show qos description
config qos average-data-rate
config qos burst-data-rate
config qos average-realtime-rate
config qos burst-realtime-rate

config qos dot1p-tag

To define the maximum value (0-7) for the priority tag associated with packets that fall within the profile, use the **config qos dot1p-tag** command.

config qos dot1p-tag {**bronze** | **silver** | **gold** | **platinum**} *dot1p_tag*

Syntax Description

bronze	Specifies the QoS 802.1p tag for the queue bronze.
silver	Specifies the QoS 802.1p tag for the queue silver.
gold	Specifies the QoS 802.1p tag for the queue gold.
platinum	Specifies the QoS 802.1p tag for the queue platinum.
<i>dot1p_tag</i>	Dot1p tag value between 1 and 7.

Command Default

None.

Examples

This example shows how to configure the a QoS 802.1p tag for the queue gold with the dot1p tag value of 5:

```
> config qos dot1p-tag gold 5
```

Related Commands

show qos queue_length all
config qos protocol-type

config qos priority

To define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN, use the **config qos priority** command.

config qos priority {**bronze** | **silver** | **gold** | **platinum**} {*maximum-priority* | *default-unicast-priority* | *default-multicast-priority*}

Syntax Description

bronze	Specifies a Bronze profile of the WLAN.
silver	Specifies a Silver profile of the WLAN.
gold	Specifies a Gold profile of the WLAN.
platinum	Specifies a Platinum profile of the WLAN.
<i>maximum-priority</i>	Maximum QoS priority as one of the following: • besteffort • background • video • voice
<i>default-unicast-priority</i>	Default unicast priority as one of the following: • besteffort • background • video • voice
<i>default-multicast-priority</i>	Default multicast priority as one of the following: • besteffort • background • video • voice

Usage Guidelines

The maximum priority level should not be lower than the default unicast and multicast priority levels.

Examples

This 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.

```
> config qos priority gold voice video besteffort
```

Related Commands

`config qos protocol-type`

config qos protocol-type

To define the maximum value (0-7) 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.
<i>dot1p</i>	Specifies when dot1p type protocol is assigned.

Command Default

None.

Examples

This example shows how to configure the QoS protocol type silver:

```
> 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.
<i>queue_length</i>	Maximum queue length values (10 to 255).

Command Default

None.

Examples

This example shows how to configure the QoS length for the queue “gold” with the maximum queue length value as 12:

```
> config qos queue_length gold 12
```

Related Commands

show qos

Configure SNMP Commands

Use the **config snmp** commands to configure Simple Network Management Protocol (SNMP) settings.

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.
<i>name</i>	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

Examples

This example shows how to configure read/write access mode for SNMP community:

```
> 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

<i>name</i>	SNMP community name of up to 16 characters.

Command Default

None.

Usage Guidelines

Use this command to create a new community with the default configuration.

Examples

This example shows how to create a new SNMP community named test:

```
> 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

<i>name</i>	SNMP community name.

Command Default

None.

Examples

This example shows how to delete an SNMP community named test:

```
> 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 IP address of an SNMP community, use the **config snmp community ipaddr** command.

config snmp community ipaddr *ip_address ip_mask name*

Syntax Description

<i>ip_address</i>	SNMP community IP address.
<i>ip_mask</i>	SNMP community subnet mask.
<i>name</i>	SNMP community name.

Command Default

None.

Examples

This example shows how to configure an SNMP community with the IP address 10.10.10.10, IP mask 255.255.255.0, and SNMP community named public:

```
> config snmp community ipaddr 10.10.10.10 255.255.255.0 public
```

Related Commands

show snmp community
config snmp community mode
config snmp community accessmode
config snmp community create
config snmp community delete

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.
<i>name</i>	SNMP community name.

Command Default

None.

Examples

This example shows how to enable the SNMP community named public:

```
> config snmp community mode enable 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

<i>engine_id</i>	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.

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.

Examples

This example shows how to configure the SNMP engine ID with the value ffffffff:

```
> config snmp engineID ffffffff
```

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

<i>contact</i>	SNMP system contact name. The contact can be up to 31 alphanumeric characters.

Command Default

None.

Examples

This example shows how to set the SMNP system contact named Cisco WLAN Solution_administrator:

```
> config snmp syscontact Cisco WLAN Solution_administrator
```

Related Commands

show snmpcommunity

config snmp syslocation

To configure the SNMP system location name, use the **config snmp syslocation** command.

config snmp syslocation *location*

Syntax Description

<i>location</i>	SNMP system location name. The location can be up to 31 alphanumeric characters.

Command Default

None.

Examples

This example shows how to configure the SNMP system location name to Building_2a:

```
> config snmp syslocation Building_2a
```

Related Commands

show snmpcommunity

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_address*

Syntax Description

<i>name</i>	SNMP community name. The name contain up to 16 characters.
<i>ip_address</i>	SNMP community IP address.

Command Default

None.

Usage Guidelines

The IP address must be valid for the command to add the new server.

Examples

This example shows how to add a new SNMP trap receiver with the SNMP community named test and IP address 10.1.1.1:

```
> config snmp trapreceiver create test 10.1.1.1
```

Related Commands

show snmp trap

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

<i>name</i>	SNMP community name. The name can contain up to 16 characters.

Command Default

None.

Examples

This example shows how to delete a server named test from the SNMP trap receiver list:

```
> 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.
<i>name</i>	SNMP community name.

Command Default

None.

Usage Guidelines

This command enables or disables the Cisco wireless LAN controller from sending the traps to the selected server.

Examples

This example shows how to disable an SNMP trap receiver from sending traps to a server named server1:

```
> config snmp trapreceiver mode disable server1
```

Related Commands

show snmp trap

config snmp v3user create

To create a version 3 SNMP user, use the **config snmp v3user create** command.

config snmp v3user create *username* {**ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des** | **aescfb128**} [*auth_key*] [*encrypt_key*]

Syntax Description

<i>username</i>	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.
<i>auth_key</i>	(Optional) Authentication key for the HMAC-MD5 or HMAC-SHA authentication protocol.
<i>encrypt_key</i>	(Optional) Encryption key for the CBC-DES or CFB-AES-128 encryption protocol.

Command Default

SNMP v3 username AccessMode Authentication Encryption

----- Read/Write ----- HMAC-SHA ----- CFB-AES

default

Read/Write

HMAC-SHA

CFB-AES

Examples

This example shows how to add an SNMP username named test with read-only privileges and no encryption or authentication:

```
> 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

<i>username</i>	Username to delete.

Command Default

None.

Examples

This example shows how to remove an SNMP user named test:

```
> 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

All versions enabled.

Examples

This example shows how to enable SNMP version v1:

```
> config snmp version v1 enable
```

Related Commands

show snmpversion

Configure Trap Flag Commands

Use the **config trapflags** commands to configure trap flags settings.

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-SecuritywepDecryptError {enable | disable}

Syntax Description

enable	Enables sending 802.11 security-related traps.
disable	Disables sending 802.11 security-related traps.

Command Default

Enabled.

Examples

This example shows how to disable the 802.11 security related traps:

```
> 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

Enabled.

Examples

This example shows how to enable the sending of AAA server-related traps:

```
> 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.

Examples

This example shows how to enable trap notifications when a rogue access point is detected at the adjacent channel:

```
> 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

Enabled.

Examples

This example shows how to prevent traps from sending access point-related traps:

```
> 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

Enabled.

Examples

This example shows how to prevent sending traps on invalid SNMP access:

```
> 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

Disabled.

Examples

This example shows how to enable the sending of Dot11 disassociation trap to clients:

```
> 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

90.

Usage Guidelines

Table 3: Maximum Number of Clients Supported on Different Controllers

Controller	Maximum number of supported clients
Cisco 5500 Series Controllers	7000
Cisco 2500 Series Controllers	500
Cisco Wireless Services Module 2	15000
Cisco Flex 7500 Series Controllers	64000
Cisco 8500 Series Controllers	64000
Cisco Virtual Wireless LAN Controllers	30000

Examples

This example shows how to configure the threshold value of the number of clients that associate with the 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

Enabled.

Examples

This example shows how to enable the sending of configuration-saved traps:

```
> config trapflags configsave enable
```

Related Commands

show trapflags

config trapflags IPsec

To enable or disable the sending of IPsec traps, use the **config trapflags IPsec** command.

config trapflags IPsec {esp-auth | esp-reply | invalidSPI | ike-neg | suite-neg | invalid-cookie} {enable | disable}

Syntax Description

esp-auth	Enables the sending of IPsec traps when an ESP authentication failure occurs.
esp-reply	Enables the sending of IPsec traps when an ESP replay failure occurs.
invalidSPI	Enables the sending of IPsec traps when an ESP invalid SPI is detected.
ike-neg	Enables the sending of IPsec traps when an IKE negotiation failure occurs.
suite-neg	Enables the sending of IPsec traps when a suite negotiation failure occurs.
invalid-cookie	Enables the sending of IPsec traps when a Isakamp invalid cookie is detected.
enable	Enables sending of IPsec traps.
disable	Disables sending of IPsec traps.

Command Default

Enabled.

Examples

This example shows how to enable the sending of IPsec traps when ESP authentication failure occurs:

```
> config trapflags IPsec esp-auth enable
```

Related Commands

show trapflags

config trapflags linkmode

To enable or disable Cisco wireless LAN controller level link up/down trap flags, use the **config trapflags linkmode** command.

config trapflags linkmode {enable | disable}

Syntax Description

enable	Enables Cisco wireless LAN controller level link up/down trap flags.
disable	Disables Cisco wireless LAN controller level link up/down trap flags.

Command Default

Enabled.

Examples

This example shows how to enable the Cisco wireless LAN controller level link up/down trap:

```
> config trapflags linkmode disable
```

Related Commands

show trapflags

config trapflags mesh

To configure trap notifications when a mesh access point is detected, use the **config trapflags mesh** command.

config trapflags mesh {enable | disable}

Syntax Description

enable	Enables trap notifications when a mesh access point is detected.
disable	Disables trap notifications when a mesh access point is detected.

Command Default

None.

Examples

This example shows how to enable trap notifications when a mesh access point is detected:

```
> config trapflags mesh enable
```

Related Commands

config trapflags 802.11-Security
config trapflags aaa
config trapflags ap
config trapflags adjchannel-rogueap
config trapflags authentication
config trapflags client
config trapflags configsave
config trapflags IPsec
config trapflags linkmode
config trapflags multiusers
config trapflags strong-pwdcheck
config trapflags rfid
config trapflags rogueap
show trapflags

config trapflags multiusers

To enable or disable the sending of traps when multiple logins are active, use the **config trapflags multiusers** command.

config trapflags multiusers {enable | disable}

Syntax Description

enable	Enables the sending of traps when multiple logins are active.
disable	Disables the sending of traps when multiple logins are active.

Command Default

Enabled.

Examples

This example shows how to disable the sending of traps when multiple logins are active:

```
> config trapflags multiusers disable
```

Related Commands

show trapflags

config trapflags rfid

To configure the threshold value of the maximum number of RFID tags, after which an SNMP trap and a syslog message is sent to the controller, use the **config trapflags rfid** command.

config trapflags rfid {**threshold** | **enable** | **disable**}

Syntax Description

threshold	Configures the threshold percentage value of the maximum number of RFID tags, after which an SNMP trap and a syslog message is sent to the controller. The range is from 80 to 100. The traps and syslog messages are generated every 10 minutes. You cannot configure this interval.
enable	Enables the generation of the traps and syslog messages.
disable	Disables the generation of the traps and syslog messages.

Command Default

90.

Usage Guidelines

The table below shows the maximum number of RFID tags supported on different controllers:

Table 4: Maximum Number of RFID Tags Supported on Different Controllers

Controller	Maximum number of supported clients
Cisco 5500 Series Controllers	5000
Cisco 2500 Series Controllers	500
Cisco Wireless Services Module 2	10000
Cisco Flex 7500 Series Controllers	50000
Cisco 8500 Series Controllers	50000
Cisco Virtual Wireless LAN Controllers	3000

Examples

This example shows how to configure the threshold value of the maximum number of RFID tags:

```
> config trapflags rfid 80
```

Related Commands

config trapflags 802.11-Security
config trapflags aaa
config trapflags ap

config trapflags adjchannel-rogueap
config trapflags authentication
config trapflags client
config trapflags configsave
config trapflags IPsec
config trapflags linkmode
config trapflags multiusers
config trapflags mesh
config trapflags strong-pwdcheck
config trapflags rogueap
config trapflags mesh
show trapflags

config trapflags rogueap

To enable or disable sending rogue access point detection traps, use the **config trapflags rogueap** command.

config trapflags rogueap {enable | disable}

Syntax Description

enable	Enables the sending of rogue access point detection traps.
disable	Disables the sending of rogue access point detection traps.

Command Default

Enabled

Examples

This example shows how to disable the sending of rogue access point detection traps:

```
> 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

Enabled.

Examples

This example shows how to enable the sending of RRM parameter-related traps:

```
> 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

Enabled.

Examples

This example shows how to disable the sending of RRM profile-related traps:

```
> config trapflags rrm-profile load disable
```

Related Commands

show trapflags

config trapflags stpmode

To enable or disable the sending of spanning tree traps, use the **config trapflags stpmode** command.

config trapflags stpmode {enable | disable}

Syntax Description

enable	Enables the sending of spanning tree traps.
disable	Disables the sending of spanning tree traps.

Command Default

Enabled.

Examples

This example shows how to disable the sending of spanning tree traps:

```
> config trapflags stpmode disable
```

Related Commands

show trapflags

config trapflags strong-pwdcheck

To configure trap notifications for strong password checks, use the **config trapflags strong-pwdcheck** command.

config trapflags strong-pwdcheck {enable | disable}

Syntax Description

enable	Enables trap notifications for strong password checks.
disable	Disables trap notifications for strong password checks.

Command Default

None.

Examples

This example shows how to enable trap notifications for strong password checks:

```
> config trapflags strong-pwdcheck enable
```

Related Commands

config trapflags 802.11-Security
config trapflags aaa
config trapflags ap
config trapflags adjchannel-rogueap
config trapflags authentication
config trapflags client
config trapflags configsave
config trapflags IPsec
config trapflags linkmode
config trapflags multiusers
config trapflags mesh
config trapflags rfid
config trapflags rogueap
show trapflags

config trapflags wps

To enable or disable Wireless Protection System (WPS) trap sending, use the **config trapflags wps** command.

config trapflags wps {enable | disable}

Syntax Description

enable	Enables WPS trap sending.
disable	Disables WPS trap sending.

Command Default

Enabled.

Examples

This example shows how to disable the WPS traps sending:

```
> config trapflags wps disable
```

Related Commands

show trapflags

Other Config Commands

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

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

Primary.

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.

Examples

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

```
> config boot primary
```

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

```
> 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.
<i>seconds</i>	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.
<i>holdtime_interval</i>	Maximum hold timer value. The range is from 10 to 255 seconds.

Command Default

The default value for CDP timer is 60 seconds.

The default value for CDP holdtime is 180 seconds.

Examples

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

```
> 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.

Examples

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

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

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

```
> config certificate compatibility
```

Related Commands

config certificate lsc
show certificate compatibility
show certificate lsc
show certificate summary
show local-auth certificates

config certificate lsc

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

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

Syntax Description

enable	Enables LSC certificates on the controller.
disable	Disables LSC certificates on the controller.
ca-server	Specifies the Certificate Authority (CA) server settings.
<i>http://url:port/path</i>	Domain name or IP address of the CA server.
ca-cert	Specifies CA certificate database settings.
add	Obtains a CA certificate from the CA server and adds it to the controller's certificate database.
delete	Deletes a CA certificate from the controller's certificate database.
subject-params	Specifies the device certificate settings.
<i>country state city orgn dept email</i>	Country, state, city, organization, department, and email of the certificate authority. Note The common name (CN) is generated automatically on the access point using the current MIC/SSC format <i>Cxxxx-MacAddr</i> , where <i>xxxx</i> is the product number.
other-params	Specifies the device certificate key size settings.
<i>keysize</i>	Value from 384 to 2048 (in bits); the default value is 2048.
ap-provision	Specifies the access point provision list settings.
auth-list	Specifies the provision list authorization settings.
<i>ap_mac</i>	MAC address of access point to be added or deleted from the provision list.
revert-cert	Specifies the number of times the access point attempts to join the controller using an LSC before reverting to the default certificate.
<i>retries</i>	Value from 0 to 255; the default value is 3. Note If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate. If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Command Default

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

Usage Guidelines

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

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

Examples

This example shows how to enable the LSC settings:

```
> config certificate lsc enable
```

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

```
> config certificate lsc ca-server http://10.0.0.1:8080/caserver
```

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

```
> config certificate lsc ca-cert add
```

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

```
> config certificate lsc keysize 2048
```

Related Commands

config certificate

show certificate compatibility

show certificate lsc

show certificate summary

show local-auth certificates

config certificate ssc

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

config certificate ssc hash validation {enable | disable}

Syntax Description

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

Command Default

Enabled.

Usage Guidelines

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

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

Examples

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

```
> config certificate ssc hash validation enable
```

Related Commands

show certificate ssc
show mobility group member
config mobility group member hash
config certificate
show certificate compatibility
show certificate lsc
show certificate summary
show local-auth certificates

config certificate use-device-certificate webadmin

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

config certificate use-device-certificate webadmin

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to use a device certificate for web administration:

```
> 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 coredump** 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.

Examples

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

```
> 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

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

Command Default

None.

Usage Guidelines

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

Examples

This 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*:

```
> 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

<i>ftp_username</i>	FTP server login username.

<i>ftp_password</i>	FTP server login password.

Command Default

None.

Usage Guidelines

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

Examples

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

```
> 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.

Examples

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

```
> 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

<i>URL</i>	URL used for web-based client authorization.

Command Default

None.

Examples

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

```
> 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.
<i>index</i>	Index of the external web server in the list of external web server. The index must be a number between 1 and 20.
<i>IP_address</i>	IP address of the external web server.
delete	Deletes an external web server.

Command Default

None.

Examples

This 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:

```
> 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.

Examples

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

```
> config custom-web logout-popup disable
```

Related Commands

config custom-web redirectUrl
config custom-web weblogo
config custom-web webmessage
config custom-web webtitle
config custom-web ext-webauth-url show custom-web

config custom-web redirectUrl

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

config custom-web redirectUrl *URL*

Syntax Description

<i>URL</i>	URL that is redirected to the specified address.

Command Default

None.

Examples

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

```
> config custom-web redirectUrl abc.com
```

Related Commands

- config custom-web weblogo**
- config custom-web webmessage**
- config custom-web webtitle**
- config custom-web ext-webauth-mode**
- config custom-web ext-webauth-url**
- show custom-web**

config custom-web webauth-type

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

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

Syntax Description

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

Command Default

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

Examples

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

```
> 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.

Examples

This example shows how to enable the web authentication logo:

```
> 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

<i>message</i>	Message text for web authentication.

Command Default

None.

Examples

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

```
> 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

<i>title</i>	Custom title text for web authentication.

Command Default

None.

Examples

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

```
> config custom-web webtitle Helpdesk
```

Related Commands

- config custom-web redirectUrl**
- config custom-web weblogo**
- config custom-web webmessage**
- config custom-web ext-webauth-mode**
- config custom-web ext-webauth-url**
- show custom-web**

config dhcp

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

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

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

Syntax Description

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

netbios-name-server <i>scope wins1 [wins2] [wins3]</i>	Configures the netbios name servers. You must specify the scope name and the IP address of a name server. Optionally, you can specify the IP addresses of secondary and tertiary name servers.
network <i>scope network netmask</i>	Configures the network and netmask. You must specify the scope name, the network address, and the network mask.
opt-82 remote-id	Configures the DHCP option 82 remote ID field format. DHCP option 82 provides additional security when DHCP is used to allocate network addresses. The controller acts as a DHCP relay agent to prevent DHCP client requests from untrusted sources. The controller adds option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.
<i>ap_mac</i>	MAC address of the access point to the DHCP option 82 payload.
<i>ap_mac:ssid</i>	MAC address and SSID of the access point to the DHCP option 82 payload.
<i>ap-ethmac</i>	Remote ID format as AP Ethernet MAC address.
<i>apname:ssid</i>	Remote ID format as AP name:SSID.
<i>ap-group-name</i>	Remote ID format as AP group name.
<i>flex-group-name</i>	Remote ID format as FlexConnect group name .
<i>ap-location</i>	Remote ID format as AP location.
<i>apmac-vlan_id</i>	Remote ID format as AP radio MAC address:VLAN_ID.
<i>apname-vlan_id</i>	Remote ID format as AP Name:VLAN_ID.
<i>ap-ethmac-ssid</i>	Remote ID format as AP Ethernet MAC:SSID address.

Command Default

The default values for ap-group-name is "default-group", and for ap-location is "default location".
If ap-group-name and flex-group-name are null, then the system MAC is sent as the remote ID field.

Usage Guidelines

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

Examples

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

```
> config dhcp lease 003
```

Related Commands

- config dhcp proxy**
- config dhcp timeout**
- config interface dhcp**
- config wlan dhcp_server**
- debug dhcp**
- debug dhcp service-port**
- debug disable-all**
- show dhcp**
- show dhcp proxy**

config dhcp proxy

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

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

Syntax Description

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

Command Default

Enabled.

Usage Guidelines

Follow these guidelines when you use this command:

- Use the **show dhcp proxy** command to display the status of DHCP proxy handling.
- To enable third-party WGB support, you must enable the passive-client feature on the wireless LAN by entering the **config wlan passive-client enable** command.

Examples

This example shows how to disable the DHCP packet modification:

```
> config dhcp proxy disable
```

This example shows how to enable the DHCP BootP broadcast option:

```
> config dhcp proxy disable bootp-broadcast enable
```

Related Commands

config dhcp
config dhcp timeout
config interface dhcp
config wlan dhcp_server
debug dhcp
debug dhcp service-port
debug disable-all
show dhcp
show dhcp proxy

config dhcp timeout

To configure a DHCP timeout, use the **config dhcp timeout** command.

config dhcp timeout *timeout-value*

Syntax Description

<i>timeout-value</i>	Timeout value in the range of 5 to 120 seconds.

Command Default

None.

Examples

This example shows how to set the DHCP timeout to 10 seconds:

```
> config dhcp timeout 10
```

Related Commands

- config dhcp proxy
- config dhcp timeout
- config interface dhcp
- config wlan dhcp_server
- debug dhcp
- debug dhcp service-port
- debug disable-all
- show dhcp
- show dhcp proxy

config flow

To configure the NetFlow monitor and exporter, use the **config flow** command.

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

Syntax Description

add	Associates a NetFlow monitor with an exporter, or a NetFlow record with a NetFlow monitor.
delete	Dissociates a NetFlow monitor from an exporter, or a NetFlow record from a NetFlow monitor.
monitor	Configures a NetFlow monitor.
<i>monitor_name</i>	Name of the NetFlow monitor. The monitor name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces for a monitor name.
exporter	Configures a NetFlow exporter.
<i>exporter_name</i>	Name of the NetFlow exporter. The exporter name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces for an exporter name.
record	Associates a NetFlow record to the NetFlow monitor.
<i>record_name</i>	Name of the IPv4 NetFlow record of the client application.

Command Default

None.

Usage Guidelines

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

Examples

This example shows how to configure the flow monitor and exporter:

```
> config flow add monitor monitor1 exporter exporter1
```

Related Commands

show flow exporter
show flow monitor
config wlan flow

config license agent

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

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

Syntax Description

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

Command Default

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

The listener is **disabled** by default.

Notify is **disabled** by default.

The default maximum number of sessions is 9.

The default maximum message size is 0.

Usage Guidelines

If your network contains various Cisco licensed devices, you might consider using the CLM to manage all of the licenses using a single application. CLM is a secure client/server application that manages Cisco software licenses network wide.

The license agent is an interface module that runs on the controller and mediates between CLM and the controller's licensing infrastructure. CLM can communicate with the controller using various channels, such as HTTP, Telnet, and so on. If you want to use HTTP as the communication method, you must enable the license agent on the controller.

The license agent receives requests from the CLM and translates them into license commands. It also sends notifications to the CLM. It uses XML messages over HTTP or HTTPS to receive the requests and send the notifications. For example, if the CLM sends a **license clear** command, the agent notifies the CLM after the license expires.



Note

You can download the CLM software and access user documentation at this URL: <http://www.cisco.com/en/US/products/ps7138/index.html>

Examples

This example shows how to authenticate the default license agent settings:

```
> config license agent default authenticate
```

This example shows how to configure the license agent with the number of maximum sessions allowed as 5:

```
> config license agent max-session 5
```

Related Commands

license install

show license agent

clear license agent

config license boot

To specify the license level to be used on the next reboot of the Cisco 5500 Series Controller, use the **config license boot** command.

config license boot {base | wplus | auto}

Syntax Description

base	Specifies the base boot level.
wplus	Specifies the wplus boot level.
auto	Specifies the auto boot level.

Command Default

None.

Usage Guidelines

If you enter **auto**, the licensing software automatically chooses the license level to use on the next reboot. It generally chooses permanent licenses over evaluation licenses and wplus licenses over base licenses.



Note

If you are considering upgrading from a base license to a wplus license, you can try an evaluation wplus license before upgrading to a permanent wplus license. To activate the evaluation license, you need to set the image level to wplus in order for the controller to use the wplus evaluation license instead of the base permanent license.



Note

To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

Examples

This example shows how to set the license boot settings to wplus:

```
> config license boot wplus
```

Related Commands

license install
show license in-use
license modify priority

config load-balancing

To globally configure aggressive load balancing on the controller, use the **config load-balancing** command.

config load-balancing {**window** *client_count* | **status** {**enable** | **disable**} | **denial** *denial_count*}

config load-balancing uplink-threshold *traffic_threshold*

Syntax Description

window	Specifies the aggressive load balancing client window.
<i>client_count</i>	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.
<i>denial_count</i>	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.
<i>traffic_threshold</i>	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

Disabled.

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

Examples

This example shows how to enable the aggressive load-balancing settings:

```
> 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 {**add** *location* [*description*] | **delete** *location* | **enable** | **disable** | **description** *location* *description* | **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

add	Adds a location element.
<i>location</i>	Location element name.
<i>description</i>	Element description. Optional with the add command, and required with the description command.
delete	Deletes a location element.
enable	Enables the access point location-based overrides.
disable	Disables the access point location-based overrides.
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.
<i>seconds</i>	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.
<i>threshold</i>	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.
<i>wlan_id</i>	WLAN identification name.
<i>interface_name</i>	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.
<i>burst_interval</i>	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.

Examples

This example shows how to specify the simple algorithm for averaging RSSI and SNR values on a location-based controller:

```
> config location algorithm simple
```

Related Commands

clear location rfid
clear location statistics rfid
show location
show location statistics rfid

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.

Examples

This example shows how to set the controller buffer severity level for logging messages to 4:

```
> 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.

Examples

This example shows how to set the controller console severity level for logging messages to 3:

```
> 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,
The **buffered** and **syslog** commands are disabled.

Examples

This example shows how to save the debug messages to the controller console:

```
> 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.

Examples

This example shows how to enable the controller to include information about the source file in the message logs:

```
> 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.

Examples

This example shows how to enable the controller to include the process information in the message logs:

```
> 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.

Examples

This example shows how to disable the controller to include the traceback information in the message logs:

```
> 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 *host_IP_address*

Syntax Description

<i>host_IP_address</i>	IP address for the remote host.

Command Default

None.

Usage Guidelines

To remove a remote host that was configured for sending syslog messages, enter the **config logging syslog host** *host_IP_address* **delete** command.

Examples

This example shows how to configure a remote host 10.92.125.52 for sending the syslog messages:

```
> config logging syslog host 10.92.125.52
```

Related Commands

config logging syslog facility
config logging syslog level
show logging

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.

Examples

This example shows how to set the facility for outgoing syslog messages to authorization:

```
> config logging syslog facility authorization
```

Related Commands

config logging syslog host

config logging syslog level

show logging

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.

Examples

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

```
> 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

<i>session_id</i>	ID of the session to close.
all	Closes all Telnet sessions.

Command Default

None.

Examples

This example shows how to close all active Telnet sessions:

```
> config loginsession close all
```

Related Commands

show loginsession

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.
<i>interval</i>	Time interval. The range is from 1 to 30 seconds.

Command Default

None.

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.

Examples

This example shows how to modify the NMSP notification interval for the active RFID tags to 25 seconds:

```
> 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

Enabled.

Examples

This example shows how to enable scrolling of the page

```
> 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

Disabled.

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.

Examples

This example shows how to enable display of passwords in plain text:

```
> 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

<i>prompt</i>	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.

Usage Guidelines

Because the system prompt is a user-defined variable, it is omitted from the rest of this documentation.

Examples

This example shows how to change the CLI system prompt to Cisco 4400:

```
> config prompt "Cisco 4400"
```

config rfid auto-timeout

To configure an automatic timeout of radio frequency identification (RFID) tags, use the **config rfid auto-timeout** command.

config rfid auto-timeout {enable | disable}

Syntax Description

enable	Enables an automatic timeout.
disable	Disables an automatic timeout.

Command Default

None.

Examples

This example shows how to enable an automatic timeout of RFID tags:

```
> config rfid auto-timeout enable
```

Related Commands

show rfid summary
config rfid status
config rfid timeout

config rfid status

To configure radio frequency identification (RFID) tag data tracking, use the **config rfid status** command.

config rfid status {enable | disable}

Syntax Description

enable	Enables RFID tag tracking.
disable	Enables RFID tag tracking.

Command Default

None.

Examples

This example shows how to configure RFID tag tracking settings:

```
> config rfid status enable
```

Related Commands

show rfid summary
config rfid auto-timeout
config rfid timeout

config rfid timeout

To configure a static radio frequency identification (RFID) tag data timeout, use the **config rfid timeout** command.

config rfid timeout *seconds*

Syntax Description	
	<i>seconds</i> Timeout in seconds (from 60 to 7200).

Command Default	
	None.

Examples	
	This example shows how to configure a static RFID tag data timeout of 60 seconds.
	<pre>> config rfid timeout 60</pre>

Related Commands	
	show rfid summary
	config rfid statistics

config service timestamps

To enable or disable timestamps in message logs, use the **config service timestamps** command.

config service timestamps {**debug** | **log**} {**datetime** | **disable**}

Syntax Description

debug	Configures timestamps in debug messages.
log	Configures timestamps in log messages.
datetime	Specifies to timestamp message logs with the standard date and time.
disable	Specifies to prevent message logs being timestamped.

Command Default

Disabled.

Examples

This example shows how to configure timestamp message logs with the standard date and time:

```
> config service timestamps log datetime
```

This example shows how to prevent message logs being timestamped:

```
> 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

<i>session_num</i>	Number of sessions from 0 to 5.

Command Default

5.

Usage Guidelines

Up to five sessions are possible while a setting of zero prohibits any Telnet CLI sessions.

Examples

This example shows how to configure the number of allowed CLI sessions to 2:

```
> 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

<i>timeout</i>	Timeout of Telnet session in minutes (from 0 to 160). A value of 0 indicates no timeout.

Command Default

5.

Examples

This example shows how to configure the inactivity timeout for Telnet sessions to 20 minutes:

```
> config sessions timeout 20
```

Related Commands

show sessions

config switchconfig boot-break

To enable or disable the breaking into boot prompt by pressing the Esc key at system startup, use the **config switchconfig boot-break** command.

config switchconfig boot-break {enable | disable}

Syntax Description

enable	Enables the breaking into boot prompt by pressing the Esc key at system startup.
disable	Disables the breaking into boot prompt by pressing the Esc key at system startup.

Command Default

Disabled.

Usage Guidelines

You must enable the features that are prerequisites for the Federal Information Processing Standard (FIPS) mode before enabling or disabling the breaking into boot prompt.

Examples

This example shows how to enable the breaking into boot prompt by pressing the Esc key at system startup:

```
> config switchconfig boot-break enable
```

Related Commands

show switchconfig
config switchconfig flowcontrol
config switchconfig mode
config switchconfig secret-obfuscation
config switchconfig fips-prerequisite
config switchconfig strong-pwd

config switchconfig fips-prerequisite

To enable or disable the features that are prerequisites for the Federal Information Processing Standard (FIPS) mode, use the **config switchconfig fips-prerequisite** command.

config switchconfig fips-prerequisite {enable | disable}

Syntax Description

enable	Enables the features that are prerequisites for the FIPS mode.
disable	Disables the features that are prerequisites for the FIPS mode.

Command Default

Disabled.

Usage Guidelines

You must configure the FIPS authorization secret before you can enable or disable the FIPS prerequisite features.

Examples

This example shows how to enable the features that are prerequisites for the FIPS mode:

```
> config switchconfig fips-prerequisite enable
```

Related Commands

show switchconfig
config switchconfig flowcontrol
config switchconfig mode
config switchconfig secret-obfuscation
config switchconfig boot-break
config switchconfig strong-pwd

config switchconfig strong-pwd

To enable or disable your controller to check the strength of newly created passwords, use the **config switchconfig strong-pwd** command.

config switchconfig strong-pwd {**case-check** | **consecutive-check** | **default-check** | **username-check** | **all-checks**} {**enable** | **disable**}

Syntax Description

case-check	Checks at least three combinations: lowercase characters, uppercase characters, digits, or special characters.
consecutive-check	Checks the occurrence of the same character three times.
default-check	Checks for default values or use of their variants.
username-check	Checks whether the username is specified or not.
all-checks	Checks all cases.
enable	Enables a strong password check for the AP and controller.
disable	Disables a strong password check for the AP and controller.

Command Default

Enabled.

Examples

This example shows how to enable the case check feature of the strong password check:

```
> config switchconfig strong-pwd case-check enable
```

Related Commands

show switchconfig
config switchconfig flowcontrol
config switchconfig mode
config switchconfig secret-obfuscation
config switchconfig fips-prerequisite
config switchconfig boot-break

config switchconfig flowcontrol

To enable or disable 802.3x flow control, use the **config switchconfig flowcontrol** command.

config switchconfig flowcontrol {enable | disable}

Syntax Description

enable	Enables 802.3x flow control.
disable	Disables 802.3x flow control.

Command Default

Disabled.

Examples

This example shows how to enable 802.3x flow control on Cisco wireless LAN controller parameters:

```
> config switchconfig flowcontrol enable
```

Related Commands

show switchconfig

config switchconfig mode

To configure Lightweight Access Port Protocol (LWAPP) transport mode for Layer 2 or Layer 3, use the **config switchconfig mode** command.

config switchconfig mode {L2 | L3}

Syntax Description

L2	Specifies Layer 2 as the transport mode.
L3	Specifies Layer 3 as the transport mode.

Command Default

L3

Examples

This example shows how to configure LWAPP transport mode to Layer 3:

```
> config switchconfig mode L3
```

Related Commands

show switchconfig

config switchconfig secret-obfuscation

To enable or disable secret obfuscation, use the **config switchconfig secret-obfuscation** command.

config switchconfig secret-obfuscation {enable | disable}

Syntax Description

enable	Enables secret obfuscation.
disable	Disables secret obfuscation.

Command Default

Secrets and user passwords are obfuscated in the exported XML configuration file.

Usage Guidelines

To keep the secret contents of your configuration file secure, do not disable secret obfuscation. To further enhance the security of the configuration file, enable configuration file encryption.

Examples

This example shows how to enable secret obfuscation:

```
> config switchconfig secret-obfuscation enable
```

Related Commands

show switchconfig

config sysname

To set the Cisco wireless LAN controller system name, use the **config sysname** command.

config sysname *name*

Syntax Description

<i>name</i>	System name. The name can contain up to 31 alphanumeric characters.

Command Default

None.

Examples

This example shows how to configure the system named Ent_01:

```
> config sysname Ent_01
```

Related Commands

show sysinfo

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.

Examples

This example shows how to configure the system date to 04/04/2010 and time to 15:29:00:

```
> 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** *seconds*} | {**key-auth** {**add** *key_index* **md5** {**ascii** | **hex**} *key_value* | **delete** *key_index*} } } | {**server** *server_index* *ip-address*}

Syntax Description

auth	Configures the NTP authentication.
enable	Enables the NTP authentication.
<i>server_index</i>	NTP server index.
<i>key_index</i>	Key index between 1 and 4294967295.
disable	Disables the NTP authentication.
interval	Configures the NTP polling interval.
<i>seconds</i>	NTP polling interval in seconds (between 3600 and 604800).
key-auth	Configures the NTP authentication key.
add	Adds an NTP authentication key.
md5	Specifies the authentication protocol.
ascii	Specifies the ASCII key format (a maximum of 16 characters).
hex	Specifies the hexadecimal key format (a maximum of 32 digits).
delete	Deletes an authentication key.
server	Configures the NTP servers.
<i>ip_address</i>	NTP server's IP address. Use 0.0.0.0 to delete the entry.

Command Default

None.

Examples

This example shows how to configure the NTP polling interval to 7000 seconds:

```
> config time ntp interval 7000
```

This example shows how to enable NTP authentication where the server index is 4 and the key index is 1:

```
> config time ntp auth enable 4 1
```

This 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:

```
> config time ntp key-auth add 1 md5 hex ff
```

This 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:

```
> config time ntp key-auth add 1 md5 ascii ciscokey
```

Related Commands **show ntp-keys**

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.
<i>delta_hours</i>	Local hour difference from the Universal Coordinated Time (UCT).
<i>delta_mins</i>	Local minute difference from UCT.

Command Default

None.

Examples

This example shows how to enable the daylight saving time:

```
> 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, Jakarta
- (GMT +8:00) Hong Kong, Beijing, Chongqing
- (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.

Examples

This example shows how to set the location of the time zone in order to set the daylight saving time to location index 10 automatically:

```
> config time timezone location 10
```

Related Commands

show time

config wlan flow

To associate a NetFlow monitor with a WLAN, use the **config wlan flow** command.

config wlan flow *wlan_id* **monitor** *monitor_name* {**enable** | **disable**}

Syntax Description		
	<i>wlan_id</i>	Wireless LAN identifier from 1 to 512 (inclusive).
	monitor	Configures a NetFlow monitor.
	<i>monitor_name</i>	Name of the NetFlow monitor. The monitor name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces for a monitor name.
	enable	Associates a NetFlow monitor with a WLAN.
	disable	Dissociates a NetFlow monitor from a WLAN.

Command Default None.

Usage Guidelines You can use the **config flow** command to create a new NetFlow monitor.

Examples This example shows how to associate a NetFlow monitor with a WLAN:
> **config wlan flow 5 monitor monitor1 enable**

Related Commands

- show flow exporter**
- show flow monitor**
- config flow**

Saving Configurations

Use the **save config** command before you log out of the CLI to save all previous configuration changes.

save config

To save Cisco Wireless LAN Controller configurations, use the **save config** command.

save config

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to save the Cisco wireless LAN controller settings:

```
> save config
Are you sure you want to save? (y/n) y
Configuration Saved!
```

Related Commands **show sysinfo**

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

Disabled (ignore).

Usage Guidelines

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

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

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

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

Examples

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

```
> 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:

```
> 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

Disabled (ignore).

Usage Guidelines

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

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

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

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

Examples

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

```
> 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 802.11 cac voice max-bandwidth

config 802.11 cac voice stream-size

config advanced timers ap-discovery-timeout

To configure the Cisco lightweight access point discovery time-out, use the **config advanced timers ap-discovery-timeout** command.

config advanced timers ap-discovery-timeout *seconds*

Syntax Description	<i>seconds</i> Cisco lightweight access point discovery timeout value between 1 and 10 seconds.
Command Default	10 seconds.
Usage Guidelines	The Cisco lightweight access point discovery timeout is how often a Cisco wireless LAN controller attempts to discover unconnected Cisco lightweight access points.
Examples	This example shows how to configure an access point discovery-timeout with the timeout value of 20: <pre>> config advanced timers ap-discovery-timeout 20</pre>
Related Commands	show advanced timers config advanced timers ap-heartbeat-timeout config advanced timers ap-fast-heartbeat config advanced timers ap-primary-discovery-timeout config advanced timers auth-timeout

config advanced timers ap-heartbeat-timeout

To configure the Cisco lightweight access point heartbeat timeout, use the **config advanced timers ap-heartbeat-timeout** command.

config advanced timers ap-heartbeat-timeout *seconds*

Syntax Description

<i>seconds</i>	Cisco lightweight access point heartbeat timeout value between 1 and 30 seconds.

Command Default

30 seconds.

Usage Guidelines

The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keep-alive signal to the Cisco wireless LAN controller.

This *seconds* value should be at least three times larger than the fast heartbeat timer.

Examples

This example shows how to configure an access point heartbeat timeout to 20:

```
> config advanced timers ap-heartbeat-timeout 20
```

Related Commands

show advanced timers

config advanced timers ap-discovery-timeout

config advanced timers ap-fast-heartbeat

config advanced timers ap-primary-discovery-timeout

config advanced timers auth-timeout

config advanced timers ap-primary-discovery-timeout

To configure the access point primary discovery request timer, use the **config advanced timers ap-primary-discovery-timeout** command.

config advanced timers ap-primary-discovery-timeout *interval*

Syntax Description

<i>interval</i>	Access point primary discovery request timer between 30 and 3600 seconds.

Command Default

120 seconds.

Examples

This example shows how to configure the access point primary discovery request timer to 1200 seconds:

```
> config advanced timers ap-primary-discovery-timeout 1200
```

Related Commands

show advanced timers
config advanced timers ap-discovery-timeout
config advanced timers ap-fast-heartbeat
config advanced timers ap-heartbeat-timeout
config advanced timers auth-timeout

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

<i>seconds</i>	Authentication response timeout value in seconds between 10 and 600.

Command Default

10 seconds.

Examples

This example shows how to configure the authentication timeout to 20 seconds:

```
> config advanced timers auth-timeout 20
```

Related Commands

show advanced timers

config advanced timers ap-discovery-timeout

config advanced timers ap-heartbeat-timeout

config advanced timers ap-primary-discovery-timeout

config advanced timers ap-fast-heartbeat

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

<i>seconds</i>	EAP timeout value in seconds between 8 and 120.

Command Default

None.

Examples

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

```
> config advanced timers eap-timeout 10
```

Related Commands

show advanced timers

config dhcp timeout

To configure a DHCP timeout, use the **config dhcp timeout** command.

config dhcp timeout *timeout-value*

Syntax Description

<i>timeout-value</i>	Timeout value in the range of 5 to 120 seconds.

Command Default

None.

Examples

This example shows how to set the DHCP timeout to 10 seconds:

```
> config dhcp timeout 10
```

Related Commands

- config dhcp proxy**
- config dhcp timeout**
- config interface dhcp**
- config wlan dhcp_server**
- debug dhcp**
- debug dhcp service-port**
- debug disable-all**
- show dhcp**
- show dhcp proxy**

config ldap

To configure the Lightweight Directory Access Protocol (LDAP) server settings, use the **config ldap** command.

config ldap {**add** | **delete** | **enable** | **disable** | **retransmit-timeout**} *index*

Syntax Description

add	Specifies that an LDAP server is being added.
delete	Specifies that an LDAP server is being deleted.
enable	Specifies that an LDAP serve is enabled.
disable	Specifies that an LDAP server is disabled.
retransmit-timeout	Changes the default retransmit timeout for an LDAP server.
<i>index</i>	LDAP server index. The range is from 1 to 17.

Command Default

None.

Examples

This example shows how to enable LDAP server index 10:

```
> config ldap enable 10
```

Related Commands

config ldap add
config ldap simple-bind
show ldap summary

config remote-lan session-timeout

To configure client session timeout, use the **config remote-lan session-timeout** command.

config remote-lan session-timeout *remote-lan-id seconds*

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>seconds</i>	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

Command Default

None.

Examples

This example shows how to configure the client session timeout to 6000 seconds for a remote LAN with ID 1:

```
> config remote-lan session-timeout 1 6000
```

Related Commands

show remote-lan

config network usertimeout

To change the timeout for idle client sessions, use the **config network usertimeout** command.

config network usertimeout *seconds*

Syntax Description	<i>seconds</i>	Timeout duration in seconds. The minimum value is 90. The default value is 300.
Command Default	300.	
Usage Guidelines	Use this command to set the idle client session duration on the Cisco wireless LAN controller. The minimum duration is 90 seconds.	
Examples	This example shows how to configure the idle session timeout to 1200 seconds: > 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

<i>index</i>	RADIUS server index.
<i>timeout</i>	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None.

Examples

This example shows how to configure retransmission timeout value 5 seconds between the retransmission:

```
> 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

<i>index</i>	RADIUS server index.
<i>retransmit-timeout</i>	Timeout value. The range is from 1 to 30 seconds.

Command Default

None.

Examples

This example shows how to configure a default RADIUS server retransmission timeout for management users:

```
> 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

<i>index</i>	RADIUS server index.
<i>timeout</i>	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None.

Examples

This example shows how to configure a retransmission timeout of 5 seconds for a RADIUS authentication server:

```
> config radius auth retransmit-timeout 5
```

Related Commands

show radius auth statistics

config radius auth server-timeout

To configure a retransmission timeout value for a RADIUS accounting server, use the **config radius auth server-timeout** command.

config radius auth server-timeout *index timeout*

Syntax Description

<i>index</i>	RADIUS server index.
<i>timeout</i>	Timeout value. The range is from 2 to 30 seconds.

Command Default

The default timeout is 2 seconds.

Examples

This example shows how to configure a server timeout value of 2 seconds for RADIUS authentication server index 10:

```
> config radius auth server-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

1200 seconds.

Examples

This example shows how to set an expiration time for entries in the rogue access point and client list to 2400 seconds:

```
> 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

<i>index</i>	TACACS+ authorization server index.
<i>timeout</i>	Timeout value. The range is 1 to 30 seconds.

Command Default

None.

Examples

This example shows how to configure a default TACACS+ authorization server timeout for management users:

```
> 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

<i>index</i>	TACACS+ authentication server index.
<i>timeout</i>	Timeout value. The range is 1 to 30 seconds.

Command Default

None.

Examples

This example shows how to configure a default TACACS+ authentication server timeout for management users:

```
> config tacacs auth mgmt-server-timeout 1 10
```

Related Commands

config tacacs auth

config rfid auto-timeout

To configure an automatic timeout of radio frequency identification (RFID) tags, use the **config rfid auto-timeout** command.

config rfid auto-timeout {enable | disable}

Syntax Description

enable	Enables an automatic timeout.
disable	Disables an automatic timeout.

Command Default

None.

Examples

This example shows how to enable an automatic timeout of RFID tags:

```
> config rfid auto-timeout enable
```

Related Commands

show rfid summary
config rfid status
config rfid timeout

config rfid timeout

To configure a static radio frequency identification (RFID) tag data timeout, use the **config rfid timeout** command.

config rfid timeout *seconds*

Syntax Description

<i>seconds</i>	Timeout in seconds (from 60 to 7200).

Command Default

None.

Examples

This example shows how to configure a static RFID tag data timeout of 60 seconds.

```
> config rfid timeout 60
```

Related Commands

show rfid summary
config rfid statistics

config wlan session-timeout

To change the timeout of wireless LAN clients, use the **config wlan session-timeout** command.

config wlan timeout {*wlan_id* | **foreignAp**} *seconds*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>seconds</i>	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

Command Default

None.

Examples

This example shows how to configure the client timeout to 6000 seconds for WLAN ID 1:

```
> config wlan session-timeout 1 6000
```

Related Commands

show wlan

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

<i>timeout</i>	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.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

300 seconds.

Usage Guidelines

The timeout value that you configure here overrides the global timeout that you define using the command **config network usertimeout**.

Examples

This example shows how to configure the idle client sessions for a WLAN:

```
> config wlan usertimeout 100 1
```

Related Commands

config network usertimeout
config wlan user-idle-threshold

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.
<i>seconds</i>	Reassociation deadline interval in seconds.
enable	Enables 802.11r fast transition 802.1X support.
disable	Disables 802.11r fast transition 802.1X support.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to configure authentication key-management using 802.11r fast transition:

```
> config wlan security wpa akm ft reassociation-timeout 25 1
```

Related Commands

show wlan

config wlan security ft

To configure 802.11r fast transition 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.
<i>timeout-in-seconds</i>	Reassociation timeout value in seconds. The valid range is 1 to 100 seconds.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

Examples

This example shows how to enable 802.11r fast transition roaming support on WLAN 2:

```
> config wlan security ft enable 2
```

This example shows how to set the reassociation timeout value of 20 seconds for 802.11r fast transition roaming support on WLAN 2:

```
> config wlan security ft reassociation-timeout 20 2
```

Related Commands

show wlan

Clearing Configurations, Log files, and Other Actions

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

clear acl counters

To clear the current counters for an access control list (ACL), use the **clear acl counters** command.

clear acl counters *acl_name*

Syntax Description

<i>acl_name</i>	ACL name.

Command Default

None.

Usage Guidelines

Note

ACL counters are available only on the following controllers: Cisco 4400 Series Controller, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

Examples

This example shows how to clear the current counters for acl1:

```
> clear acl counters acl1
```

Related Commands

config acl counter
show acl

clear ap-config

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

clear ap-config *ap_name*

Syntax Description

<i>ap_name</i>	Access point name.

Command Default

None.

Usage Guidelines

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

Examples

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

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

Related Commands

show ap config

clear ap-eventlog

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

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

Syntax Description

specific	Specifies a specific access point log file.
<i>ap_name</i>	Name of the access point for which the event log file will be emptied.
all	Deletes the event log for all access points joined to the controller.

Command Default

None.

Examples

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

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

Related Commands

show ap eventlog

clear ap join stats

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

clear ap join stats {all | *ap_mac*}

Syntax Description

all	Specifies all access points.
<i>ap_mac</i>	Access point MAC address.

Command Default

None.

Examples

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

```
> clear ap join stats all
```

Related Commands

show ap config

clear arp

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

clear arp

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to clear the ARP table:

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

Related Commands

clear transfer
clear download datatype
clear download filename
clear download mode
clear download serverip
clear download start
clear upload datatype
clear upload filename
clear upload mode
clear upload path
clear upload serverip
clear upload start
clear stats port

clear avc statistics

To clear AVC statistics of a client, guest LAN, remote LAN, or a WLAN use the **clear avc statistics** command.

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

Syntax Description

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

Command Default

None.

Examples

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

```
> clear avc statistics client 00:21:1b:ea:36:60
```

Related Commands

config avc profile create
config avc profile delete
config avc profile rule
config wlan avc
show avc profile
show avc applications

show avc statistics

debug avc error

debug avc events

clear client tsm

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

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

Syntax Description

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

Command Default

None.

Examples

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

```
> 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.

Examples

This example shows how to reset the configuration data to factory defaults:

```
> 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.

Examples This example shows how to clear the external web authentication URL:

```
> clear ext-webauth-url
URL cleared.
```

Related Commands

- clear transfer
- clear download datatype
- clear download filename
- clear download mode
- clear download serverip
- clear download start
- clear upload datatype
- clear upload filename
- clear upload mode
- clear upload path
- clear upload serverip
- clear upload start
- clear stats port

clear license agent

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

clear license agent {counters | sessions}

Syntax Description

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

Command Default None.

Examples

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

```
> clear license agent counters
```

Related Commands

config license agent
show license agent
license install

clear location rfid

To clear a specific radio frequency identification (RFID) tag or all of the RFID tags in the entire database, use the **clear location rfid** command.

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

Syntax Description

<i>mac_address</i>	MAC address of a specific RFID tag.
all	Specifies all of the RFID tags in the database.

Command Default

None.

Examples

This example shows how to clear all of the RFID tags in the database:

```
> clear location rfid all
```

Related Commands

clear location statistics rfid
config location
show location
show location statistics rfid

clear location statistics rfid

To clear radio frequency identification (RFID) statistics, use the **clear location statistics rfid** command.

clear location statistics rfid

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to clear RFID statistics:

```
> clear location statistics rfid
```

Related Commands

- config location**
- show location**
- show location statistics rfid**

clear loep statistics

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

clear loep statistics

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to clear the statistics related to LOCP:

```
> clear loep statistics
```

Related Commands

- clear nmosp statistics**
- config nmosp notify-interval measurement**
- show nmosp notify-interval summary**
- show nmosp statistics**
- show nmosp 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.

Examples	This example shows how to clear the login banner file:

> **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.

Usage Guidelines

This command is executed from 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 IOS Release 12.3(11)JX1 or higher releases.

Examples

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

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

Related Commands

debug capwap
debug capwap reap
debug lwapp console cli
show capwap reap association
show capwap reap status

clear mdns service-database

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

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

Syntax Description	all	Clears the mDNS service database.
	<i>service-name</i>	Name of the mDNS service. The controller clears the details of the mDNS service.

Command Default None.

Usage Guidelines The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database.

Examples This example shows how to clear the mDNS service database:
> **clear mdns service-database all**

Related Commands

- config mdns query interval**
- config mdns service**
- config mdns snooping**
- config interface mdns-profile**
- config interface group mdns-profile**
- config wlan mdns**
- show mdns profile**
- show mnds service**
- config mdns profile**
- debug mdns all**
- debug mdns error**
- debug mdns detail**
- debug mdns message**

clear nmsp statistics

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

clear nmsp statistics

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to delete the NMSP statistics log file:

```
> clear nmsp statistics
```

Related Commands

- clear loep 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.

Examples

This example shows how to clear the RADIUS accounting statistics:

```
> 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.

Examples

This example shows how to clear the RADIUS authentication server statistics:

```
> 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.

Examples	This example shows how to clear the custom web authentication redirect URL:

```
> 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.

Examples

This example shows how to clear the WLAN configuration elements of the access point *cisco_ap*:

```
> clear stats ap wlan cisco_ap  
WLAN statistics cleared.
```

Related Commands

show ap stats

show ap wlan

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.

Examples This example shows how to clear the local EAP statistics:

```
> clear stats local-auth
Local EAP Authentication Stats Cleared.
```

Related Commands

- config local-auth active-timeout**
- config local-auth eap-profile**
- config local-auth method fast**
- config local-auth user-credentials**
- debug aaa local-auth**
- show local-auth certificates**
- show local-auth config**
- show local-auth statistics**

clear stats mobility

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

clear stats mobility

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to clear mobility manager statistics:

```
> clear stats mobility
Mobility stats 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 stats port

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

clear stats port *port*

Syntax Description

<i>port</i>	Physical interface port number.

Command Default

None.

Examples

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

```
> clear stats port 9
```

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 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.

Examples

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

```
> clear stats radius auth all
```

Related Commands

clear transfer
clear download datatype
clear download filename
clear download mode
clear download serverip
clear download start
clear upload datatype
clear upload filename
clear upload mode
clear upload path
clear upload serverip
clear upload start
clear stats port

clear stats switch

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

clear stats switch

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to clear all switch statistics counters:

```
> clear stats switch
```

Related Commands

- clear transfer
- clear download datatype
- clear download filename
- clear download mode
- clear download path
- clear download start
- clear upload datatype
- clear upload filename
- clear upload mode
- clear upload path
- clear upload serverip
- clear upload start

clear stats tacacs

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

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

Syntax Description

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

Command Default

None.

Examples

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

```
> 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.

Examples This example shows how to clear the transfer information:

```
> 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.

Examples This example shows how to clear the trap log:

```
> 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.

Examples This example shows how to clear the custom web authentication image:

```
> 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.

Examples This example shows how to clear the custom web authentication message:

```
> 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.

Examples This example shows how to clear the custom web authentication title:

```
> 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.
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.

Examples

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

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

Related Commands

reset system notify-time
reset system in

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.
no-swap	Boots from the active image.
reset-aps	Resets all access points during the system reset.
save-config	Saves the configuration before the system reset.

Command Default

None.

Examples

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

```
> reset system in 00:01:01 image swap reset-aps save-config
```

Related Commands

reset system notify-time
reset system at

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.

Examples	This example shows how to cancel a scheduled reset:

```
> reset system cancel
```

Related Commands	reset system at reset system in reset system notify-time

reset system notify-time

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

reset system notify-time *minutes*

Syntax	Description
<i>minutes</i>	Number of minutes before each scheduled reset at which to generate a trap.

Command Default	Description
The default is 10 minutes.	

Examples	Description
<pre>> reset system notify-time 55</pre>	This example shows how to configure the trap generation to 10 minutes before the scheduled resets:

Related Commands	Description
reset system in	
reset system at	

reset peer-system

To reset the peer controller, use the **reset peer-system** command.

reset peer-system

Syntax Description	This command has no arguments or keywords.

Command Default	None.

Examples	This example shows how to reset the peer controller: > reset peer-system

Related Commands	reset system notify-time reset system in

Uploading and Downloading Files and Configurations

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

transfer download certpassword

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

<i>private_key_password</i>	Certificate's private key password.

Command Default

None.

Examples

This example shows how to transfer a file to the switch with the certificate's private key password certpassword:

```
> transfer download certpassword  
Clearing password
```

Related Commands

clear transfer
transfer download filename
transfer download mode
transfer download path
transfer download serverip
transfer download start
transfer upload datatype
transfer upload filename
transfer upload mode
transfer upload path
transfer upload serverip
transfer upload start

transfer download datatype

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

transfer download datatype {**config** | **code** | **image** | **signature** | **webadmincert** | **webauthbundle** | **eapdevcert** | **eapcacert**}

Syntax Description

config	Downloads the configuration file.
code	Downloads an executable image to the system.
image	Downloads a web page login to the system.
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.
eapdevcert	Downloads an EAP dev certificate to the system.
eapcacert	Downloads an EAP ca certificate to the system.

Command Default

None.

Examples

This example shows how to download an executable image to the system:

```
> transfer download datatype code
```

Related Commands

clear transfer
transfer download filename
transfer download mode
transfer download path
transfer download serverip
transfer download start
transfer upload filename
transfer upload mode
transfer upload path
transfer upload serverip
transfer upload start

transfer download filename

To download a specific file, use the **transfer download filename** command.

transfer download filename *filename*

Syntax Description

<i>filename</i>	Filename that contains up to 512 alphanumeric characters.

Command Default

None.

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the filename.

Examples

This example shows how to transfer a file named build603:

```
> transfer download filename build603
```

Related Commands

- clear transfer
- transfer download certpassword
- transfer download mode
- transfer download path
- transfer download serverip
- transfer download start
- transfer upload datatype
- transfer upload certpassword
- transfer upload mode
- transfer upload path
- transfer upload serverip
- transfer upload start

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.

Examples

This example shows how to transfer a file using the TFTP mode:

```
> transfer download mode tftp
```

Related Commands

clear transfer
transfer download filename
transfer download certpassword
transfer download path
transfer download serverip
transfer download start
transfer upload datatype
transfer upload filename
transfer upload path
transfer upload serverip
transfer upload start

transfer download password

To set the password for an FTP transfer, use the **transfer download password** command.

transfer download password *password*

Syntax Description

<i>password</i>	Password.

Command Default

None.

Examples

This example shows how to set the password for FTP transfer to pass01:

```
> transfer download password pass01
```

Related Commands

transfer download mode
transfer download port
transfer download username

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.

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the file path.

Examples

This example shows how to transfer a file to the path c:\install\version2:

```
> transfer download path c:\install\version2
```

Related Commands

clear transfer
 transfer download filename
 transfer download mode
 transfer download certpassword
 transfer download serverip
 transfer download start
 transfer upload datatype
 transfer upload filename
 transfer upload mode
 transfer upload path
 transfer upload serverip
 transfer upload start

transfer download port

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

transfer download port *port*

Syntax Description

<i>port</i>	FTP port.

Command Default

The default FTP *port* is 21.

Examples

This example shows how to specify FTP port number 23:

```
> transfer download port 23
```

Related Commands

transfer download mode

transfer download path

transfer download username

transfer download serverip

To configure the IP address of the TFTP server from which to download information, use the **transfer download serverip** command.

transfer download serverip *TFTP_server* *ip_address*

Syntax Description

<i>TFTP_server</i>	TFTP IP address.
<i>ip_address</i>	Server IP address.

Command Default

None.

Examples

This example shows how to configure the IP address of the TFTP server with the IP address 175.34.56.78:

```
> transfer download serverip 175.34.56.78
```

Related Commands

clear transfer
transfer download filename
transfer download mode
transfer download path
transfer download serverip
transfer download start
transfer upload datatype
transfer upload filename
transfer upload mode
transfer upload path
transfer upload serverip
transfer upload start
clear transfer
transfer download filename
transfer download mode
transfer download path
transfer download certpassword
transfer download start
transfer upload datatype

transfer upload filename

transfer upload mode

transfer upload path

transfer upload serverip

transfer upload start

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.

Examples This example shows how to initiate a download:

```
> 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 Commands

- clear transfer**
- transfer download filename**
- transfer download mode**
- transfer download path**
- transfer download serverip**
- transfer download certpassword**
- transfer upload datatype**
- transfer upload filename**
- transfer upload mode**
- transfer upload path**
- transfer upload serverip**
- transfer upload start**

transfer download tftpPktTimeout

To specify the TFTP packet timeout, use the **transfer download tftpPktTimeout** command.

transfer download tftpPktTimeout *timeout*

Syntax	Description
<i>timeout</i>	Timeout in seconds between 1 and 254.

Command Default
None.

Examples
This example shows how to transfer a file with the TFTP packet timeout of 55 seconds: <pre>> transfer download tftpPktTimeout 55</pre>

Related Commands
clear transfer transfer download filename transfer download mode transfer download path transfer download serverip transfer download start transfer upload datatype transfer upload filename transfer upload mode transfer upload path transfer upload serverip transfer upload start

transfer download tftpMaxRetries

To specify the number of allowed TFTP packet retries, use the **transfer download tftpMaxRetries** command.

transfer download tftpMaxRetries *retries*

Syntax Description

<i>retries</i>	Number of allowed TFTP packet retries between 1 and 254 seconds.

Command Default

None.

Examples

This example shows how to set the number of allowed TFTP packet retries to 55:

```
> transfer download tftpMaxRetries 55
```

Related Commands

- clear transfer**
- transfer download filename**
- transfer download mode**
- transfer download path**
- transfer download serverip**
- transfer download start**
- transfer upload datatype**
- transfer upload filename**
- transfer upload mode**
- transfer upload path**
- transfer upload serverip**
- transfer upload start**

transfer download username

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

transfer download username *username*

Syntax Description

<i>username</i>	Username.

Command Default

None.

Examples

This example shows how to set the FTP username to ftp_username:

```
> transfer download username ftp_username
```

Related Commands

transfer download mode

transfer download path

transfer download password

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.
<i>key</i>	Encryption key for config file transfers.

Command Default

None.

Examples

This example shows how to enable the encryption settings:

```
> transfer encrypt enable
```

Related Commands

clear transfer
transfer download filename
transfer download mode
transfer download path
transfer download serverip
transfer download start
transfer upload datatype
transfer upload filename
transfer upload mode
transfer upload path
transfer upload serverip
transfer upload start

transfer upload datatype

To set the controller to upload specified log and crash files, use the **transfer upload datatype** command.

transfer upload datatype {config | coredump | crashfile | errorlog | invalid-config | pac | packet-capture | panic-crash-file | radio-core-dump | signature | systemtrace | traplog | watchdog-crash-file}

Syntax Description

config	Uploads the system configuration file.
coredump	Uploads the core-dump file.
crashfile	Uploads the system crash file.
errorlog	Uploads the system error log file.
invalid-config	Uploads the system invalid-config file.
pac	Uploads a Protected Access Credential (PAC).
packet-capture	Uploads a packet capture file.
panic-crash-file	Uploads the kernel panic information file.
radio-core-dump	Uploads the system error log.
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.

Command Default

None.

Examples

This example shows how to upload the system error log file:

```
> transfer upload datatype errorlog
```

Related Commands

clear transfer
transfer upload filename
transfer upload mode

transfer upload pac
transfer upload password
transfer upload path
transfer upload port
transfer upload serverip
transfer upload start
transfer upload username

transfer upload filename

To upload a specific file, use the **transfer upload filename** command.

transfer upload filename *filename*

Syntax Description

<i>filename</i>	Filename that contains up to 16 alphanumeric characters.

Command Default

None.

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the filename.

Examples

This example shows how to upload a file build603:

```
> transfer upload filename build603
```

Related Commands

- clear transfer**
- transfer upload datatype**
- transfer upload mode**
- transfer upload pac**
- transfer upload password**
- transfer upload path**
- transfer upload port**
- transfer upload serverip**
- transfer upload start**
- transfer upload username**

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.

Examples

This example shows how to set the transfer mode to TFTP:

```
> transfer upload mode tftp
```

Related Commands

clear transfer
transfer upload filename
transfer upload datatype
transfer upload pac
transfer upload password
transfer upload path
transfer upload port
transfer upload serverip
transfer upload start
transfer upload username

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

<i>username</i>	User identity of the PAC.
<i>validity</i>	Validity period (days) of the PAC.
<i>password</i>	Password to protect the PAC.

Command Default

None.

Usage Guidelines

The client upload process uses a TFTP or FTP server.

Examples

This example shows how to upload a PAC with the username user1, validity period 53, and password pass01:

```
> transfer upload pac user1 53 pass01
```

Related Commands

clear transfer
transfer upload filename
transfer upload mode
transfer upload datatype
transfer upload password
transfer upload path
transfer upload port
transfer upload serverip
transfer upload start
transfer upload username

transfer upload password

To configure the password for FTP transfer, use the **transfer upload password** command.

Syntax Description

<i>password</i>	Password needed to access the FTP server.

transfer upload password *password*

Command Default

None.

Examples

This example shows how to configure the password for the FTP transfer to pass01:

```
> transfer upload password pass01
```

Related Commands

- clear transfer**
- transfer upload filename**
- transfer upload mode**
- transfer upload pac**
- transfer upload datatype**
- transfer upload path**
- transfer upload port**
- transfer upload serverip**
- transfer upload start**
- transfer upload username**

transfer upload path

To set a specific upload path, use the **transfer upload path** command.

transfer upload path *path*

Syntax Description

<i>path</i>	Server path to file.

Command Default

None.

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the file path.

Examples

This example shows how to set the upload path to c:\install\version2:

```
> transfer upload path c:\install\version2
```

Related Commands

clear transfer
transfer upload filename
transfer upload mode
transfer upload pac
transfer upload password
transfer upload datatype
transfer upload port
transfer upload serverip
transfer upload start
transfer upload username

transfer upload peer-start

To upload a file to the peer controller, use the **transfer upload peer-start** command.

transfer upload peer-start

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to start uploading a file to the peer controller:

```
> transfer upload peer-start
Mode..... FTP
FTP Server IP..... 209.165.201.1
FTP Server Port..... 21
FTP Path..... /builds/nimm/
FTP Filename..... AS_5500_7_4_1_20.aes
FTP Username..... wnbu
FTP Password..... *****
Data Type..... Error Log

Are you sure you want to start upload from standby? (y/N) n

Transfer Canceled
```

Related Commands

- clear transfer
- transfer upload filename
- transfer upload mode
- transfer upload pac
- transfer upload password
- transfer upload path
- transfer upload port
- transfer upload serverip
- transfer upload datatype
- transfer upload username

transfer upload port

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

transfer upload port *port*

Syntax Description

<i>port</i>	Port number.

Command Default

The default FTP port is 21.

Examples

This example shows how to specify FTP port 23:

```
> transfer upload port 23
```

Related Commands

- clear transfer**
- transfer upload filename**
- transfer upload mode**
- transfer upload pac**
- transfer upload password**
- transfer upload path**
- transfer upload datatype**
- transfer upload serverip**
- transfer upload start**
- transfer upload username**

transfer upload serverip

To configure the IP address of the TFTP server to upload files to, use the **transfer upload serverip** command.

transfer upload serverip *ip_address*

Syntax Description

<i>ip_address</i>	Server IP address.

Command Default

None.

Examples

This example shows how to set the IP address of the TFTP server to 175.31.56.78:

```
> transfer upload serverip 175.31.56.78
```

Related Commands

- clear transfer**
- transfer upload filename**
- transfer upload mode**
- transfer upload pac**
- transfer upload password**
- transfer upload path**
- transfer upload port**
- transfer upload datatype**
- transfer upload start**
- transfer upload username**

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.

Examples	This example shows how to initiate an upload of a file:

```
> 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 Commands	clear transfer
	transfer upload filename
	transfer upload mode
	transfer upload pac
	transfer upload password
	transfer upload path
	transfer upload port
	transfer upload serverip
	transfer upload datatype
	transfer upload username

transfer upload username

To specify the FTP username, use the **transfer upload username** command.

transfer upload username

Syntax Description

<i>username</i>	Username required to access the FTP server. The username can contain up to 31 characters.

Command Default

None.

Examples

This example shows how to set the FTP username to ftp_username:

```
> transfer upload username ftp_username
```

Related Commands

- clear transfer**
- transfer upload filename**
- transfer upload mode**
- transfer upload pac**
- transfer upload password**
- transfer upload path**
- transfer upload port**
- transfer upload serverip**
- transfer upload start**
- transfer upload datatype**

Installing and Modifying Licenses on Cisco 5500 Series Controllers

Use the **license** commands to install, remove, modify, or rehost licenses.



Note

Some license commands are available only on the Cisco 5500 Series Controller. Right to Use (RTU) licensing is not supported on Cisco 5500 Series Controllers.

**Note**

For detailed information on installing and rehosting licenses on the Cisco 5500 Series Controller, see the “Installing and Configuring Licenses” section in Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide*.

license clear

To remove a license from the Cisco 5500 Series Controller, use the **license clear** command.

license clear *license_name*

Syntax Description

<i>license_name</i>	Name of the license.

Command Default

None.

Usage Guidelines

You can delete an expired evaluation license or any unused license. You cannot delete unexpired evaluation licenses, the permanent base image license, or licenses that are in use by the controller.

Examples

This example shows how to remove the license settings of the license named wplus-ap-count:

```
> license clear wplus-ap-count
```

Related Commands

- license comment**
- license install**
- license revoke**
- license save**
- show license all**

license comment

To add comments to a license or delete comments from a license on the Cisco 5500 Series Controller, use the **license comment** command.

license comment {**add** | **delete**} *license_name comment_string*

Syntax Description

add	Adds a comment.
delete	Deletes a comment.
<i>license_name</i>	Name of the license.
<i>comment_string</i>	License comment.

Command Default

None.

Examples

This example shows how to add a comment “wplus ap count license” to the license name wplus-ap-count:

```
> license comment add wplus-ap-count Comment for wplus ap count license
```

Related Commands

license clear
license install
license revoke
license save
show license all

license install

To install a license on the Cisco 5500 Series Controller, use the **license install** command.

license install *url*

Syntax Description

<i>url</i>	URL of the TFTP server (tftp://server_ip/path/filename).

Command Default

None.

Usage Guidelines

We recommend that the access point count be the same for the base-ap-count and wplus-ap-count licenses installed on your controller. If your controller has a base-ap-count license of 100 and you install a wplus-ap-count license of 12, the controller supports up to 100 access points when the base license is in use but only a maximum of 12 access points when the wplus license is in use.

You cannot install a wplus license that has an access point count greater than the controller's base license. For example, you cannot apply a wplus-ap-count 100 license to a controller with an existing base-ap-count 12 license. If you attempt to register for such a license, an error message appears indicating that the license registration has failed. Before upgrading to a wplus-ap-count 100 license, you would first have to upgrade the controller to a base-ap-count 100 or 250 license.

Examples

This example shows how to install a license on the controller from the URL tftp://10.10.10.10/path/license.lic:

```
> license install tftp://10.10.10.10/path/license.lic
```

Related Commands

license clear
license install
license revoke
license save
show license all

license modify priority

To raise or lower the priority of the base-ap-count or wplus-ap-count evaluation license on a Cisco 5500 Series Controller, use the **license modify priority** command.

license modify priority *license_name* {**high** | **low**}

Syntax Description

<i>license_name</i>	Ap-count evaluation license.
high	Modifies the priority of an ap-count evaluation license.
low	Modifies the priority of an ap-count evaluation license.

Command Default

None.

Usage Guidelines

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 50 access point count and want to try an evaluation license with a 100 access point count, you can try out the evaluation license for 60 days.

AP-count evaluation licenses are set to low priority by default so that the controller uses the ap-count permanent license. If you want to try an evaluation license with an increased access point count, you must change its priority to high. If you no longer want to have this higher capacity, you can lower the priority of the ap-count evaluation license, which forces the controller to use the permanent license.



Note

You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.



Note

If the ap-count evaluation license is a wplus license and the ap-count permanent license is a base license, you must also change the feature set to wplus.



Note

To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

Examples

This example shows how to set the priority of the wplus-ap-count to high:

```
> license modify priority wplus-ap-count high
```

Related Commands

- license clear
- license install
- license revoke
- license save
- show license all

license revoke

To rehost a license on a Cisco 5500 Series Controller, use the **license revoke** command.

license revoke {*permission_ticket_url* | **rehost** *rehost_ticket_url*}

Syntax Description

<i>permission_ticket_url</i>	URL of the TFTP server (tftp://server_ip/path/filename) where you saved the permission ticket.
rehost	Specifies the rehost license settings.
<i>rehost_ticket_url</i>	URL of the TFTP server (tftp://server_ip/path/filename) where you saved the rehost ticket.

Command Default

None.

Usage Guidelines

Before you revoke a license, save the device credentials by using the **license save credential url** command. You can rehost all permanent licenses except the permanent base image license. Evaluation licenses and the permanent base image license cannot be rehosted.

In order to rehost a license, you must generate credential information from the controller and use it to obtain a permission ticket to revoke the license from the Cisco licensing site (www.cisco.com/go/license). Next, you must obtain a rehost ticket and use it to obtain a license installation file for the controller on which you want to install the license.

For detailed information on rehosting licenses, see the “Installing and Configuring Licenses” section in Chapter 4 of the Cisco Wireless LAN Controller Configuration Guide.

Examples

This example shows how to revoke the license settings from the saved permission ticket URL tftp://10.10.10.10/path/permit_ticket.lic:

```
> license revoke tftp://10.10.10.10/path/permit_ticket.lic
```

This example shows how to revoke the license settings from the saved rehost ticket URL tftp://10.10.10.10/path/rehost_ticket.lic:

```
> license revoke rehost tftp://10.10.10.10/path/rehost_ticket.lic
```

Related Commands

license clear
license install
license modify priority
license save
show license all

license save

To save a backup copy of all installed licenses or license credentials on the Cisco 5500 Series Controller, use the **license save** command.

license save *credential url*

Syntax Description

<i>credential</i>	Device credential information.
<i>url</i>	URL of the TFTP server (tftp://server_ip/path/filename).

Command Default

None.

Usage Guidelines

Save the device credentials before you revoke the license by using the **license revoke** command.

Examples

This example shows how to save a backup copy of all installed licenses or license credentials on tftp://10.10.10.10/path/cred.lic:

```
> license save credential tftp://10.10.10.10/path/cred.lic
```

Related Commands

license clear
license install
license revoke
license modify priority
show license all

Configure Right to Use (RTU) Licensing Commands

Use the **license** commands to configure RTU licensing on Cisco Flex 7500 Series and 8500 Series controllers. This feature allows you to enable an AP license count on the controller without using any external tools after accepting an End User License Agreement (EULA).

license activate ap-count eval

To activate an evaluation access point license on the Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license activate ap-count eval** command.

license activate ap-count eval

Syntax Description This command has no arguments or keywords.

Command Default By default, in release 7.3 Cisco Flex 7500 Series Controllers and Cisco 8500 Series Wireless LAN Controllers support 6000 APs.

Usage Guidelines When you activate this license, the controller prompts you to accept or reject the End User License Agreement (EULA) for the given license. If you activate a license that supports a smaller number of APs than the current number of APs connected to the controller, the activation command fails.

Examples This example shows how to activate an evaluation AP-count license on a Cisco Flex 7500 Series controller:

```
> license activate ap-count eval
```

Related Commands

- license activate feature
- license add ap-count
- license add feature
- license deactivate feature
- license deactivate ap-count
- license delete ap-count
- license delete feature
- show license all
- show license evaluation
- show license feature
- show license summary
- show license detail
- show license statistics

license activate feature

To activate a feature license on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license activate feature** command.

license activate feature *license_name*

Syntax Description

<i>license_name</i>	Name of the feature license. The license name can be up to 50 case-sensitive characters.

Command Default

None.

Examples

This example shows how to activate a data DTLS feature license on a Cisco Flex 7500 Series controller:

```
> license activate feature data-DTLS
```

Related Commands

- license activate ap-count eval**
- license add ap-count**
- license add feature**
- license deactivate feature**
- license deactivate ap-count**
- license delete ap-count**
- license delete feature**
- show license all**
- show license evaluation**
- show license feature**
- show license summary**
- show license detail**
- show license statistics**

license add ap-count

To configure the number of access points (APs) that an AP license can support on Cisco Flex 7500 and 8500 Series Wireless LAN controllers, use the **license add ap-count** command.

license add ap-count *count*

Syntax Description

<i>count</i>	Number of APs that the AP license supports. The range is from 1 to the maximum number of APs that the controller can support. The count must be a multiple of 5.

Command Default

None.

Usage Guidelines

Right to Use (RTU) licensing allows you to enable a desired AP license count on the controller after accepting the End User License Agreement (EULA). You can now easily add AP counts on a controller without using external tools. RTU licensing is available only on Cisco Flex 7500 and 8500 series Wireless LAN controllers.

You can use this command to increase the count of an existing AP license. When you activate a license that supports a smaller number of APs than the current number of APs connected to the controller, the activation command fails.

Examples

This example shows how to configure the count of an AP license on a Cisco Flex 7500 Series controller:

```
> license add ap-count 5000
```

Related Commands

- license activate feature**
- license activate ap-count eval**
- license add feature**
- license deactivate feature**
- license deactivate ap-count**
- license delete ap-count**
- license delete feature**
- show license all**
- show license evaluation**
- show license feature**
- show license summary**
- show license detail**
- show license statistics**

license add feature

To add a license for a feature on the Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN controllers, use the **license add feature** command.

license add feature *license_name*

Syntax Description

<i>license_name</i>	Name of the feature license. The license name can be up to 50 case-sensitive characters. For example, data_DTLS.

Command Default

None.

Examples

This example shows how to add a DTLS feature license on a Cisco Flex 7500 Series controller:

```
> license add feature data_DTLS
```

Related Commands

- license add ap-count**
- license activate feature**
- license activate ap-count eval**
- license deactivate feature**
- license deactivate ap-count**
- license delete ap-count**
- license delete feature**
- show license all**
- show license evaluation**
- show license feature**
- show license summary**
- show license detail**
- show license statistics**

license deactivate ap-count eval

To deactivate an evaluation access point license on the Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license deactivate ap-count eval** command.

license deactivate ap-count eval

Syntax Description	This command has no arguments or keywords.

Command Default	None.

Examples	This example shows how to deactivate an evaluation AP license on a Cisco Flex 7500 Series controller: > license deactivate ap-count eval

Related Commands	license activate ap-count license activate feature license add ap-count license add feature license deactivate feature license delete ap-count license delete feature show license all show license evaluation show license feature show license summary show license detail show license statistics

license deactivate feature

To deactivate a feature license on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN controllers, use the **license deactivate feature** command.

license deactivate feature *license_name*

Syntax Description

<i>license_name</i>	Name of the feature license. The license name can be up to 50 case-sensitive characters.

Command Default

None.

Examples

This example shows how to deactivate a data DTLS feature license on a Cisco Flex 7500 Series controller:

```
> license deactivate feature data_DTLS
```

Related Commands

- license activate ap-count eval**
- license activate feature**
- license add ap-count**
- license add feature**
- license deactivate ap-count**
- license delete ap-count**
- license delete feature**
- show license all**
- show license evaluation**
- show license feature**
- show license summary**
- show license detail**
- show license statistics**

license delete ap-count

To delete an access point (AP) count license on the Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license delete ap-count** command.

license delete ap-count *count*

Syntax Description

<i>count</i>	Number of APs that the AP license supports. The range is from 1 to the maximum number of APs that the controller can support. The count must be a multiple of 5.

Command Default

None.

Examples

This example shows how to delete an AP count license on a Cisco Flex 7500 Series controller:

```
> license delete ap-count 5000
```

Related Commands

- license activate feature**
- license activate ap-count eval**
- license add ap-count**
- license add feature**
- license deactivate feature**
- license deactivate ap-count**
- license delete feature**
- show license all**
- show license evaluation**
- show license feature**
- show license summary**
- show license detail**
- show license statistics**

license delete feature

To delete a license for a feature on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN controllers, use the **license delete feature** command.

license delete feature *license_name*

Syntax Description

<i>license_name</i>	Name of the feature license.

Command Default

None.

Examples

This example shows how to delete the High Availability feature license on a Cisco Flex 7500 Series controller:

```
> license delete feature high_availability
```

Related Commands

- license activate feature**
- license activate ap-count eval**
- license add feature**
- license add ap-count eval**
- license deactivate feature**
- license deactivate ap-count**
- license delete ap-count**
- show license all**
- show license evaluation**
- show license feature**
- show license summary**
- show license detail**
- show license statistics**

Troubleshooting the Controller Settings

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

debug arp

To configure Address Resolution Protocol (ARP) debug options, use the **debug arp** command.

debug arp {all | detail | events | message} {enable | disable}

Syntax Description

all	Configures debugging of all ARP logs.
detail	Configures debugging of ARP detail messages.
error	Configures debugging of ARP errors.
message	Configures debugging of ARP messages.
enable	Enables ARP debugging.
disable	Disables ARP debugging.

Command Default

None.

Examples

This example shows how to enable ARP debug settings:

```
> debug arp error enable
```

This example shows how to disable ARP debug settings:

```
> debug arp error disable
```

Related Commands

debug disable-all
show sysinfo

debug avc error

To debug Application Visibility and Control (AVC) error, use the **debug avc error** command.

debug avc error {enable | disable}

Syntax Description

enable	Enables debug of AVC error.
disable	Disables debug of AVC error.

Command Default

Disabled.

Examples

This example shows how to enable debug of AVC error:

```
> debug avc error enable
```

Related Commands

config avc profile delete
config avc profile rule
config wlan avc
show avc profile
show avc applications
show avc statistics
debug avc events

debug avc events

To debug Application Visibility and Control (AVC) events, use the **debug avc events** command.

debug avc events {enable | disable}

Syntax Description

enable	Enables debug of AVC events.
disable	Disables debug of AVC events.

Command Default

Disabled.

Examples

This example shows how to enable debug of AVC events:

```
> debug avc events enable
```

Related Commands

config avc profile delete
config avc profile rule
config wlan avc
show avc profile
show avc applications
show avc statistics
debug avc error

debug cac

To configure Call Admission Control (CAC) debug options, use the **debug cac** command.

debug cac {all | event | packet} {enable | disable}

Syntax Description

all	Configures debugging options for all CAC messages.
event	Configures debugging options for CAC events.
packet	Configures debugging options for selected CAC packets.
kts	Configures debugging options for KTS-based CAC messages.
enable	Enables the debugging.
disable	Disables the debugging.

Command Default

Disabled.

Examples

This example shows how to enable debug CAC settings:

```
> debug cac event enable
> 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 crypto

To configure hardware cryptographic debug options, use the **debug crypto** command.

debug crypto {all | sessions | trace | warning} {enable | disable}

Syntax Description

all	Configures debugging of all hardware crypto messages.
sessions	Configures debugging of hardware crypto sessions.
trace	Configures debugging of hardware crypto sessions.
warning	Configures debugging of hardware crypto sessions.
enable	Enables the hardware cryptographic debugging.
disable	Disables the hardware cryptographic debugging setting.

Command Default

None.

Examples

This example shows how to enable the debugging of hardware crypto sessions:

```
> debug crypto sessions enable
```

Related Commands

debug disable-all
show sysinfo

debug dhcp

To configure DHCP debug options, use the **debug dhcp** command.

debug dhcp {message | packet} {enable | disable}

Syntax Description

message	Configures debugging of DHCP error messages.
packet	Configures debugging of DHCP packets.
enable	Enables the DHCP debugging.
disable	Disables the DHCP debugging.

Command Default

None.

Examples

This example shows how to enable DHCP debug settings:

```
> debug dhcp message enable
```

Related Commands

debug disable-all
config dhcp
config dhcp proxy
config interface dhcp
config wlan dhcp_server
debug dhcp service-port
show dhcp
show dhcp proxy

debug dhcp service-port

To enable or disable debugging of Dynamic Host Configuration Protocol (DHCP) packets on the service port, use the **debug dhcp service-port** command.

debug dhcp service-port {enable | disable}

Syntax Description

enable	Enables the debugging of DHCP packets on the service port.
disable	Disables the debugging of DHCP packets on the service port.

Command Default

None.

Examples

This example shows how to enable debugging of DHCP packets on a service port:

```
> debug dhcp service-port enable
```

Related Commands

debug disable-all
config dhcp
config dhcp proxy
config interface dhcp
config wlan dhcp_server
debug dhcp service-port
show dhcp
show dhcp proxy

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.

Examples	This example shows how to disable all debug messages:

```
> debug disable-all
```

debug l2age

To configure debugging of Layer 2 age timeout messages, use the **debug l2age** command.

debug l2age {enable | disable}

Syntax Description

enable	Enables Layer2 age debug settings.
disable	Disables Layer2 age debug settings.

Command Default

None.

Examples

This example shows how to enable Layer2 age debug settings:

```
> debug l2age enable
```

Related Commands

debug disable-all

debug mac

To configure MAC address debugging, use the **debug mac** command.

debug mac {**disable** | **addr** *MAC*}

Syntax Description

disable	Disables MAC debugging.
addr	Configures MAC address debugging.
<i>MAC</i>	MAC address.

Command Default

None.

Examples

This example shows how to configure MAC address debugging settings:

```
> debug mac addr 00.0c.41.07.33.a6
```

Related Commands

debug disable-all

debug mdns all

To debug all multicast DNS (mDNS) messages, details, and errors, use the **debug mdns all** command.

debug mdns all {enable | disable}

Syntax Description

enable	Enables the debug of all mDNS messages, details, and errors.
disable	Disables the debug of all mDNS messages, details, and errors.

Command Default

Disabled.

Examples

This example shows how to enable the debug of all mDNS messages, details, and errors:

```
> debug mdns all enable
```

Related Commands

config mdns profile
config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns error
debug mdns detail

debug mdns detail

To debug mDNS details, use the **debug mdns detail** command.

debug mdns detail {enable | disable}

Syntax Description

enable	Enables the debug of mDNS details.
disable	Disables the debug of mDNS details.

Command Default

Disabled.

Examples

This example shows how to enable the debug of mDNS details:

```
> debug mdns detail enable
```

Related Commands

config mdns profile
config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns all
debug mdns error

debug mdns error

To debug mDNS errors, use the **debug mdns error** command.

debug mdns error {enable | disable}

Syntax Description

enable	Enables the debug of mDNS errors.
disable	Disables the debug of mDNS errors.

Command Default

Disabled.

Examples

This example shows how to enable the debug of mDNS errors:

```
> debug mdns error enable
```

Related Commands

config mdns profile
config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns all
debug mdns detail
debug mdns message

debug mdns message

To debug mDNS messages, use the **debug mdns message** command.

debug mdns message {enable | disable}

Syntax Description

enable	Enables the debug of mDNS messages.
disable	Disables the debug of mDNS messages.

Command Default

Disabled.

Examples

This example shows how to enable the debug of mDNS messages:

```
> debug mdns message enable
```

Related Commands

config mdns profile
config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns all
debug mdns error
debug mdns detail

debug memory

To enable or disable debugging of errors or events during controller memory allocation, use the **debug memory** command.

debug memory {errors | events} {enable | disable}

Syntax Description

errors	Troubleshoots memory leak errors.
events	Troubleshoots memory leak events.
enable	Enables debugging of memory leak events.
disable	Disables debugging of memory leak events.

Command Default

Disabled.

Examples

This example shows how to enable debugging of memory leak events:

```
> debug memory events enable
```

Related Commands

config memory monitor errors
show memory monitor
config memory monitor leaks

debug nmsp

To configure 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 debugging for all NMSP messages.
connection	Configures debugging for NMSP connection events.
detail	Configures debugging for NMSP events in detail.
error	Configures debugging for NMSP error messages.
event	Configures debugging for NMSP events.
message	Configures debugging for NMSP transmit and receive messages.
packet	Configures debugging for NMSP packet events.

Command Default

None.

Examples

This example shows how to configure debugging of NMSP connection events:

```
> debug nmsp connection
```

Related Commands

clear nmsp statistics
debug disable-all
config nmsp notify-interval measurement

debug ntp

To configure debugging of the Network Time Protocol (NTP), use the **debug ntp** command.

debug ntp {detail | low | packet} {enable | disable}

Syntax Description

detail	Configures debugging of detailed NTP messages.
low	Configures debugging of NTP messages.
packet	Configures debugging of NTP packets.
enable	Enables NTP debugging.
disable	Disables NTP debugging.

Command Default

None.

Examples

This example shows how to enable NTP debug settings:

```
> debug ntp packet enable
```

Related Commands

debug disable-all

debug poe

To configure debugging of Power over Ethernet (PoE) debug options, use the **debug poe** command.

debug poe {**detail** | **message** | **error**} {**enable** | **disable**}

Syntax Description

detail	Configures debugging of PoE detail logs.
error	Configures debugging of PoE error logs.
message	Configures debugging of PoE messages.
enable	Enables the PoE debugging.
disable	Disables the PoE debugging.

Command Default

None.

Examples

This example shows how to enable PoE debug settings:

```
> debug poe message enable
```

Related Commands

debug disable-all

debug rbc

To configure Router Blade Control (RBC) debug options, use the **debug rbc** command.

debug rbc {all | detail | errors | packet} {enable | disable}

Syntax Description

all	Configures debugging of RBC.
detail	Configures debugging of RBC detail.
errors	Configures debugging of RBC errors.
packet	Configures debugging of RBC packet trace.
enable	Enables RBC debugging.
disable	Disables RBC debugging.

Command Default

None.

Examples

This example shows how to enable RBC debug settings:

```
> debug rbc packet enable
```

Related Commands

debug disable-all

debug rfid

To configure radio-frequency identification (RFID) debug options, use the **debug rfid** command.

debug rfid {all | detail | errors | nmsp | receive} {enable | disable}

Syntax Description

all	Configures debugging of all RFID.
detail	Configures debugging of RFID detail.
errors	Configures debugging of RFID error messages.
nmsp	Configures debugging of RFID Network Mobility Services Protocol (NMSP) messages.
receive	Configures debugging of incoming RFID tag messages.
enable	Enables RFID debugging.
disable	Disables RFID debugging.

Command Default

None.

Examples

This example shows how to enable debugging of RFID error messages:

```
> debug rfid errors enable
```

Related Commands

debug disable-all

debug snmp

To configure SNMP debug options, use the **debug snmp** command.

debug snmp {agent | all | mib | trap} {enable | disable}

Syntax Description

agent	Configures debugging of the SNMP agent.
all	Configures debugging of all SNMP messages.
mib	Configures debugging of the SNMP MIB.
trap	Configures debugging of SNMP traps.
enable	Enables SNMP debugging.
disable	Disables SNMP debugging.

Command Default

None.

Examples

This example shows how to enable SNMP debug settings:

```
> 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 debugging of all transfer messages.
tftp	Configures debugging of TFTP transfers.
trace	Configures debugging of transfer/upgrade.
enable	Enables transfer debugging.
disable	Disables transfer debugging.

Command Default

None.

Examples

This example shows how to enable transfer/upgrade settings:

```
> 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 voice diagnostics for voice client(s) involved in a call.
<i>client_mac1</i>	MAC address of a voice client.
<i>client_mac2</i>	(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 WCS, the verbose option is not available.
disable	Disables voice diagnostics for voice client(s) 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 client(s) is not checked.
- A few output messages of the command are sent to the WCS.
- 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.

Examples

This example shows how to enable transfer/upgrade settings:

```
> 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, use the **show debug** command.

show debug

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display if debugging is enabled:

```
> show debug
MAC debugging..... disabled
Debug Flags Enabled:
  arp error enabled.
  bcast error enabled.
```

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.

Examples This example shows how to display the event log entries:

```
> show eventlog
```

	File	Line	TaskID	Code	Time			
					d	h	m	s
EVENT>	bootos.c	788	125CEBCC	AAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125CEBCC	AAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAA	0	0	0	6
EVENT>	bootos.c	788	1216C36C	AAAAAAA	0	0	0	6
EVENT>	bootos.c	788	1216C36C	AAAAAAA	0	0	0	6
EVENT>	bootos.c	788	1216C36C	AAAAAAA	0	0	0	6
EVENT>	bootos.c	788	1216C36C	AAAAAAA	0	0	0	11

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.

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.

Examples

This example shows how to display a summary of memory monitoring settings and a summary of test results:

```
> 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.
```

This example shows how to display the monitor test results:

```
> 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 Commands

config memory monitor errors
config memory monitor leaks
debug memory

show run-config

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

show run-config [**no-ap** | **commands**]

Syntax Description	
no-ap	(Optional) Excludes access point configuration settings.
commands	(Optional) Displays a list of user-configured commands on the controller.

Command Default None.

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

Some WLAN controllers may have no Crypto Accelerator (VPN termination module) or power supplies listed because they have no provisions for VPN termination modules or power supplies.

The **show run-config** command shows only values configured by the user. It does not show system-configured default values.

Examples This example shows how to display the current controller running configuration:

```
> show run-config
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 Commands **config passwd-cleartext**

show process

To display how various processes in the system are using the CPU at that instant in time, use the **show process** command.

show process {cpu | memory}

Syntax Description

cpu	Displays how various system tasks are using the CPU at that moment.
memory	Displays the allocation and deallocation of memory from various processes in the system at that moment.

Command Default

None.

Usage Guidelines

This command is helpful in understanding if any single task is monopolizing the CPU and preventing other tasks from being performed.

Examples

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.

Examples 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
```

Configure Memory Monitor Commands

To troubleshoot hard-to-solve or hard-to-reproduce memory problems, use the **config memory monitor** commands.

**Note**

The commands in this section can be disruptive to your system and should be run only when you are advised to do so by the Cisco Technical Assistance Center (TAC).

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

Disabled by default.

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.

Examples

This example shows how to enable monitoring for memory errors and leaks for a 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

<i>low_thresh</i>	Value below which free memory cannot fall without crashing. This value cannot be set lower than 10000 KB.
<i>high_thresh</i>	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.

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.

Examples

This 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:

```
> config memory monitor leaks 12000 35000
```

Related Commands

config memory monitor leaks
debug memory

show memory monitor

Configure Message Log Level Commands

Use the **config msglog** commands to configure msglog level settings.

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.

Usage Guidelines	The message log always collects and displays critical messages, regardless of the message log level setting.

Examples	This example shows how to configure the message log severity level and display critical messages:

```
> 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.

Examples This example shows how to reset the message log to collect and display critical and noncritical error messages:

```
> 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.

Examples	This example shows how to reset the message log so that it collects and display critical, noncritical, and authentication or security-related errors:

```
> 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.

Examples This example shows how to reset the message logs so that it collects and display all messages:

```
> 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.

Examples

This 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:

```
> config msglog level warning
```

Related Commands

show msglog

