



Cisco Wireless LAN Controller Command Reference

Software Release 6.0
June 2009

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-19843-01

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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0903R)

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.

Cisco Wireless LAN Controller Command Reference
© 2009 Cisco Systems, Inc. All rights reserved.



CONTENTS

Using the ? command	1-2
Using the Help Command	1-3
Show Commands for Viewing Configuration	1-4
Show Advanced 802.11 Commands	1-9
Show Access Point Commands	1-29
Show Client Commands	1-68
Show Mesh Commands	1-152
Show Mobility Commands	1-172
Show Radius Commands	1-195
Show Radio Frequency ID Commands	1-199
Show Rogue Commands	1-203
Show TACACS Commands	1-234
Show WPS Commands	1-247
Configuring Controller Settings	1-257
Configure 802.11 Network Commands	1-257
Configure 802.11 Public Safety Commands	1-257
Configure 802.11b Commands	1-261
Configure 802.11h Commands	1-263
Configure 802.11 11n Support Commands	1-266
Configure 802.11 Antenna Commands	1-272
Configure 802.11 CAC Commands	1-279
Configure Advanced 802.11 Commands	1-319
Configure Advanced 802.11 Channel Commands	1-320
Configure Advanced 802.11 Coverage Commands	1-328
Configure Advanced 802.11 Logging Commands	1-337
Configure Advanced 802.11 Monitor Commands	1-344
Configure Advanced 802.11 Profile Commands	1-350
Configure Advanced Timers Commands	1-368
Configure Access Point Commands	1-375
Configure Client Commands	1-436
Configure Interface Commands	1-474
Configure Macfilter Commands	1-526
Configure Memory Monitor Commands	1-533
Configure Mesh Commands	1-536
Configure Management-User Commands	1-556

Configure Mobility Commands	1-560
Configure Message Log Level Commands	1-570
Configure Net User Commands	1-575
Configure Network Commands	1-589
Configure Port Commands	1-619
Configure Radius Account Commands	1-634
Configure RADIUS Authentication Server Commands	1-644
Configure Rogue Commands	1-662
Configure SNMP Commands	1-684
Configure Spanning Tree Protocol Commands	1-697
Configure TACACS Commands	1-709
Configure Trap Flag Commands	1-719
Configure Watchlist Commands	1-733
Configure Wireless LAN Commands	1-737
Configure Wireless LAN Security Commands	1-766
Configure WPS Commands	1-801
Saving Configurations	1-814
Clearing Configurations, Logfiles, and Other Actions	1-815
Uploading and Downloading Files and Configurations	1-845
Installing and Modifying Licenses	1-868
Troubleshooting Commands	1-875



Cisco Wireless LAN Controller 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.

This document covers the commands available in the Cisco CLI release 6.0. The controllers currently covered include:

- Cisco 2100, 4400, and 5500 Series Wireless LAN Controllers
- Cisco Wireless Services Modules (WiSM)
- Cisco Wireless LAN Controller Network Modules
- Catalyst 3750G Integrated Wireless LAN Controller Switches

This chapter contains the following sections:

- [Using the ? command](#)
- [Using the Help Command](#)
- [Show Commands for Viewing Configuration](#)
- [Configuring Controller Settings](#)
- [Saving Configurations](#)
- [Clearing Configurations, Logfiles, and Other Actions](#)
- [Uploading and Downloading Files and Configurations](#)
- [Installing and Modifying Licenses](#)
- [Troubleshooting Commands](#)

Using the ? command

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 **command name** and ?.

Examples

The following 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.

The following command shows you that datatype is the only entry at the transfer download level:

```
> transfer download d?
datatype
```

The following command shows you the permissible entries for the transfer download datatype command:

```
> transfer download datatype ?

config      Download Configuration File.
code        Download an executable image to the system.
image       Download a web page logo to the system.
signature   Download a signature file to the system.
webadmincert Download a certificate for web administration to the system.
webauthcert Download a web certificate for web portal to the system.
```

Using the Help Command

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

help

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
```

Show Commands for Viewing Configuration

To view Cisco Wireless LAN controller options and settings, use the **show** commands.

show 802.11

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

show 802.11{a | b | h}

Syntax Description	show	Display settings.
	802.11	802.11 network settings.
	a b h	Specifies 802.11a, 802.11b/g, or 802.11h network.

Defaults None.

Examples To display basic 802.11a network settings, enter this command:

```
> show 802.11a
```

```
802.11a Network..... Enabled
11nSupport..... Enabled
    802.11a Low Band..... Enabled
    802.11a Mid Band..... Enabled
    802.11a High Band..... Enabled
802.11a Operational Rates
    802.11a 6M Rate..... Mandatory
    802.11a 9M Rate..... Supported
    802.11a 12M Rate..... Mandatory
    802.11a 18M Rate..... Supported
    802.11a 24M Rate..... Mandatory
    802.11a 36M Rate..... Supported
    802.11a 48M Rate..... Supported
    802.11a 54M Rate..... Supported
802.11n MCS Settings:
    MCS 0..... Supported
    MCS 1..... Supported
    MCS 2..... Supported
    MCS 3..... Supported
    MCS 4..... Supported
    MCS 5..... Supported
    MCS 6..... Supported
    MCS 7..... Supported
    MCS 8..... Supported
    MCS 9..... Supported
    MCS 10..... Supported
    MCS 11..... Supported
    MCS 12..... Supported
    MCS 13..... Supported
    MCS 14..... Supported
    MCS 15..... Supported
802.11n Status:
    A-MPDU Tx ..... Enabled
        Priority 0..... Enabled
        Priority 1..... Enabled
        Priority 2..... Enabled
        Priority 3..... Enabled
        Priority 4..... Enabled
        Priority 5..... Disabled
```

```

        Priority 6..... Disabled
        Priority 7..... Enabled
        A-MSDU Tx ..... Enabled
        Rifs Tx ..... Enabled
        Guard Interval ..... Short
        Beacon Interval..... 100
        CF Pollable mandatory..... Disabled
        CF Poll Request mandatory..... Disabled
        CFP Period..... 4
        CFP Maximum Duration..... 60
        Default Channel..... 36
        Default Tx Power Level..... 1
        DTPC Status..... Enabled
        Fragmentation Threshold..... 2346
        Long Retry Limit..... 4
        Maximum Rx Life Time..... 512
        Max Tx MSDU Life Time..... 512
        Medium Occupancy Limit..... 100
        Pico-Cell Status..... Disabled
        Pico-Cell-V2 Status..... Disabled
        RTS Threshold..... 2347
        Short Retry Limit..... 7
        TI Threshold..... -50
        Legacy Tx Beamforming setting..... Enabled
        Traffic Stream Metrics Status..... Disabled
        Expedited BW Request Status..... Disabled
        EDCA profile type..... default-wmm
        Voice MAC optimization status..... Disabled
        Call Admission Control (CAC) configuration
        Voice AC - Admission control (ACM)..... Disabled
            Voice max RF bandwidth..... 75
            Voice reserved roaming bandwidth..... 6
            Voice load-based CAC mode..... Disabled
            Voice tspec inactivity timeout..... Disabled
            Video AC - Admission control (ACM)..... Disabled
            Voice Stream-Size..... 84000
            Voice Max-Streams..... 2
            Video max RF bandwidth..... Infinite
            Video reserved roaming bandwidth..... 0

```

To display basic 802.11h network settings, enter this command:

```
> show 802.11h
```

```

802.11h ..... powerconstraint : 0
802.11h ..... channelswitch : Disable
802.11h ..... channelswitch mode : 0

```

Related Commands

[show network](#)
[show network summary](#)
[show ap stats](#)
[show ap summary](#)
[show client summary](#)
[show interface](#)
[show network](#)
[show port](#)
[show wlan](#)

show aaa auth

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

show aaa auth

Syntax Description	show	Display settings.
	aaa	AAA authentication server database settings.
	auth	Specifies management authentication priority settings.

Defaults
None.

Examples

```
> show aaa auth

Management authentication server order:
  1..... local
  2..... tacacs
```

Related Commands

[config aaa auth](#)
[config aaa auth mgmt](#)

show acl

To display the access control lists (ACLs) that are configured on the controller, use the **show acl** command.

show acl { **summary** | **detailed** *acl_name* }

Syntax Description

show	Display settings.
acl	ACL configurations.
summary	Displays a summary of all ACLs configured on the controller.
detailed	Displays detailed information about a specific ACL.
<i>acl_name</i>	The ACL name up to 32 alphanumeric characters.

Defaults

None.

Examples

> **show acl summary**

```
ACL Counter Status      Enabled
-----
ACL Name                Applied
-----
acl1                    Yes
acl2                    Yes
acl3                    Yes
```

> **show acl detailed** *acl_name*

```
Source          Destination          Source Port Dest Port
I Dir IP Address/Netmask IP Address/Netmask Prot  Range Range  DSCP Action Counter
-----
1 Any 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 Any 0-65535 0-65535 0 Deny 0
2 In 0.0.0.0/0.0.0.0 200.200.200.0/ 6 80-80 0-65535 Any Permit 0
255.255.255.0
```

DenyCounter : 0



Note The Counter field increments each time a packet matches an ACL rule, and the DenyCounter field increments each time a packet does not match any of the rules.

Related Commands

[clear acl counters](#)
[config acl apply](#)
[config acl counter](#)
[config acl create](#)
[config acl cpu](#)
[config acl delete](#)
[config acl rule](#)
[config interface acl](#)
[show acl cpu](#)

show acl cpu

To display the access control lists (ACLs) configured on the central processing unit (CPU), use the **show acl cpu** command.

show acl cpu

Syntax Description	show	Display settings.
	acl	ACL configurations.
	cpu	Displays a summary of all the ACLs configured on the CPU.

Command Default	None

Examples

```
> show acl cpu
CPU Acl Name.....
Wireless Traffic..... Disabled
Wired Traffic..... Disabled
Applied to NPU..... No
```

Related Commands

[clear acl counters](#)
[config acl apply](#)
[config acl counter](#)
[config acl create](#)
[config acl cpu](#)
[config acl delete](#)
[config acl rule](#)
[config interface acl](#)
[show acl](#)

Show Advanced 802.11 Commands

Use the **show advanced 802.11** commands to display more detailed or advanced 802.11a, 802.11b/g, or other supported 802.11 network settings.

show advanced 802.11 channel

To display the automatic channel assignment configuration and statistics, use the **show advanced 802.11 channel** command.

show advanced 802.11{a | b} channel

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	channel	Channel status.

Defaults None.

Examples

> **show 802.11a channel**

```
Automatic Channel Assignment
Channel Assignment Mode..... ONCE
Channel Update Interval..... 600 seconds
Anchor time (Hour of the day)..... 15
Channel Update Count..... 0
Channel Update Contribution..... S.IU
Channel Assignment Leader..... 00:0b:85:40:90:c0
Last Run..... 501 seconds ago
DCA Sensitivity Level..... MEDIUM (20 dB)
DCA 802.11n Channel Width..... 40 MHz
Channel Energy Levels
  Minimum..... -92 dBm
  Average..... -92 dBm
  Maximum..... -92 dBm
Channel Dwell Times
  Minimum..... 0 days, 00 h 58 m 45 s
  Average..... 0 days, 00 h 58 m 45 s
  Maximum..... 0 days, 00 h 58 m 45 s
Auto-RF Allowed Channel List..... 36,40
Auto-RF Allowed Channel List..... 36,40,44,48,52,56,60,64,100,
..... 104,108,112,116,132,136,140,
..... 149,153,157,161,165,190,196
DCA Outdoor AP option..... Disabled
```

Related Commands [Configure Advanced 802.11 Commands](#)
[Show Advanced 802.11 Commands](#)

show advanced 802.11 coverage

To display the configuration and statistics for coverage hole detection, use the **show advanced 802.11 coverage** command.

show advanced 802.11{a | b} coverage

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	coverage	Coverage hole detection.

Defaults None.

Examples

```
> show advanced 802.11a coverage

Coverage Hole Detection
 802.11a Coverage Hole Detection Mode..... Enabled
 802.11a Coverage Voice Packet Count..... 100 packets
 802.11a Coverage Voice Packet Percentage..... 50%
 802.11a Coverage Voice RSSI Threshold..... -80 dBm
 802.11a Coverage Data Packet Count..... 50 packets
 802.11a Coverage Data Packet Percentage..... 50%
 802.11a Coverage Data RSSI Threshold..... -80 dBm
 802.11a Global coverage exception level..... 25 %
 802.11a Global client minimum exception lev.... 3 clients
```

Related Commands

- [Configure Advanced 802.11 Commands](#)
- [Show Advanced 802.11 Commands](#)

show advanced 802.11 group

To display 802.11a or 802.11b Cisco radio RF grouping, use the **show advanced 802.11 group** command.

show advanced 802.11{a | b} group

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	group	RF grouping values.

Defaults None.

Examples

```
> show advanced 802.11a group

Radio RF Grouping
 802.11a Group Mode..... AUTO
 802.11a Group Update Interval..... 600 seconds
 802.11a Group Leader..... xx:xx:xx:xx:xx:xx
   802.11a Group Member..... xx:xx:xx:xx:xx:xx
 802.11a Last Run..... 133 seconds ago
```

Related Commands

- [Configure Advanced 802.11 Commands](#)
- [Show Advanced 802.11 Commands](#)

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		
show		Display settings.
802.11		802.11 network settings.
a b		Specifies 802.11a or 802.11b/g network.
l2roam		Layer 2 client roaming configurations.
rf-param		Radio frequency parameters.
statistics		Layer 2 client roaming statistics.
<i>mac_address</i>		The MAC address of the client.

Defaults None.

Examples To display 802.11b layer 2 client roaming information, enter this command:

```
> 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 [Configure Advanced 802.11 Commands](#)
[Show Advanced 802.11 Commands](#)

show advanced 802.11 logging

To display 802.11a or 802.11b RF event and performance logging, use the **show advanced 802.11 logging** command.

show advanced 802.11{a | b} logging

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	logging	RF event and performance logging.

Defaults None.

Examples

```
> show advanced 802.11b logging

RF Event and Performance Logging
Channel Update Logging..... Off
Coverage Profile Logging..... Off
Foreign Profile Logging..... Off
Load Profile Logging..... Off
Noise Profile Logging..... Off
Performance Profile Logging..... Off
TxPower Update Logging..... Off
```

Related Commands

[Configure Advanced 802.11 Commands](#)
[Show Advanced 802.11 Commands](#)

show advanced 802.11 monitor

To display the 802.11a or 802.11b default Cisco radio monitoring, use the **show advanced 802.11 monitor** command.

show advanced 802.11{a | b} monitor

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	monitor	Cisco radio monitoring values.

Defaults None.

Examples

```
> show advanced 802.11b monitor

Default 802.11b AP monitoring
 802.11b Monitor Mode..... enable
 802.11b Monitor Channels..... Country channels
 802.11b AP Coverage Interval..... 180 seconds
 802.11b AP Load Interval..... 60 seconds
 802.11b AP Noise Interval..... 180 seconds
 802.11b AP Signal Strength Interval..... 60 seconds
```

Related Commands

- [Configure Advanced 802.11 Commands](#)
- [Show Advanced 802.11 Commands](#)

show advanced 802.11 profile

To display the 802.11a or 802.11b lightweight access point performance profiles, use the **show advanced 802.11 profile** command.

```
show advanced 802.11{a | b} profile {global | cisco_ap}
```

Syntax Description

show	Display settings.
advanced	Advanced configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
profile	Cisco radio performance profile.
global	All Cisco lightweight access points.
<i>cisco_ap</i>	The name of a specific Cisco lightweight access point.

Defaults

None.

Examples

```
> show advanced 802.11a profile global
```

```
Default 802.11a AP performance profiles
802.11a Global Interference threshold..... 10%
802.11a Global noise threshold..... -70 dBm
802.11a Global RF utilization threshold..... 80%
802.11a Global throughput threshold..... 1000000 bps
802.11a Global clients threshold..... 12 clients
802.11a Global coverage threshold..... 12 dB
802.11a Global coverage exception level..... 80%
802.11a Global client minimum exception lev..... 3 clients
```

```
> show advanced 802.11a profile AP1
```

```
Cisco AP performance profile not customized
```

This response indicates that the performance profile for this lightweight access point is using the global defaults and has not been individually configured.

Related Commands

[Configure Advanced 802.11 Commands](#)
[Show Advanced 802.11 Commands](#)

show advanced 802.11 receiver

To display the configuration and statistics of the 802.11a or 802.11b receiver, use the **show advanced 802.11 receiver** command.

show advanced 802.11{a | b} receiver

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	receiver	Receiver settings.

Defaults None.

Examples

```
> show advanced 802.11a receiver

802.11a Receiver Settings
RxStart   : Signal Threshold..... 15
RxStart   : Signal Lamp Threshold..... 5
RxStart   : Preamble Power Threshold..... 2
RxReStart : Signal Jump Status..... Enabled
RxReStart : Signal Jump Threshold..... 10
TxStomp   : Low RSSI Status..... Enabled
TxStomp   : Low RSSI Threshold..... 30
TxStomp   : Wrong BSSID Status..... Enabled
TxStomp   : Wrong BSSID Data Only Status..... Enabled
RxAbort   : Raw Power Drop Status..... Disabled
RxAbort   : Raw Power Drop Threshold..... 10
RxAbort   : Low RSSI Status..... Disabled
RxAbort   : Low RSSI Threshold..... 0
RxAbort   : Wrong BSSID Status..... Disabled
RxAbort   : Wrong BSSID Data Only Status..... Disabled
```

Related Commands

- [Configure Advanced 802.11 Commands](#)
- [Show Advanced 802.11 Commands](#)

show advanced 802.11 summary

To display the 802.11a or 802.11b Cisco lightweight access point name, channel, and transmit level summary, use the **show advanced 802.11 summary** command.

show advanced 802.11{a | b} summary

Syntax Description

show	Display settings.
advanced	Advanced configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
summary	Cisco lightweight access point name, channel, and transmit level settings.

Defaults

None.

Examples

> **show advanced 802.11b summary**

AP Name	MAC Address	Admin State	Operation State	Channel	TxPower
CJ-1240	00:21:1b:ea:36:60	ENABLED	UP	161	1 ()
CJ-1130	00:1f:ca:cf:b6:60	ENABLED	UP	56*	1 (*)



Note

An asterisk (*) next to a channel number or power level indicates that it is being controlled by the global algorithm settings.

Related Commands

[Configure Advanced 802.11 Commands](#)
[Show Advanced 802.11 Commands](#)

show advanced 802.11 txpower

To view the 802.11a or 802.11b automatic transmit power assignment, use the **show advanced 802.11 txpower** command.

show advanced 802.11{a | b} txpower

Syntax Description	show	Display settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	txpower	Transmit power settings.

Defaults None.

Examples

> **show advanced 802.11b txpower**

```
Automatic Transmit Power Assignment
Transmit Power Assignment Mode..... AUTO
Transmit Power Update Interval..... 600 seconds
Transmit Power Threshold..... -65 dBm
Transmit Power Neighbor Count..... 3 APs
Transmit Power Update Contribution..... SN.
Transmit Power Assignment Leader..... xx:xx:xx:xx:xx:xx
Last Run..... 384 seconds ago
```

Related Commands [Configure Advanced 802.11 Commands](#)
[Show Advanced 802.11 Commands](#)

show advanced backup-controller

To display a list of primary and secondary backup controllers, use the **show advanced backup-controller** command.

show advanced backup-controller

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	backup-controller	Display backup controller list.

Defaults

None.

Examples

```
> show advanced backup-controller

AP primary Backup Controller ..... controller 10.10.10.10
AP secondary Backup Controller ..... 0.0.0.0
```

Related Commands

[Configure Advanced 802.11 Commands](#)
[Show Advanced 802.11 Commands](#)

show advanced client-handoff

To display the number of automatic client handoffs after retries, use the **show advanced client-handoff** command.

show advanced client-handoff

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	client-handoff	Client handoff retry settings.

Defaults	None.

Examples	<pre>> show advanced client-handoff Client auto handoff after retries..... 130</pre>

Related Commands	Configure Advanced 802.11 Commands Show Advanced 802.11 Commands

show advanced dot11-padding

To display the state of over-the-air frame padding on a wireless LAN controller, use the **show advanced dot11-padding** command.

show advanced dot11-padding

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	dot11-padding	Over-the-air frame padding settings.
	enable disable	Enable or disable this command.

Examples

To view the state of over-the-air frame padding, enter this command:

> **show advanced dot11-padding**

dot11-padding..... Disabled

Related Commands

[config advanced dot11-padding](#)
[debug dot11](#)
[debug dot11 mgmt interface](#)
[debug dot11 mgmt msg](#)
[debug dot11 mgmt ssid](#)
[debug dot11 mgmt state-machine](#)
[debug dot11 mgmt station](#)

show advanced eap

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

show advanced eap

Syntax	Description
show	Display settings.
eap	Client handoff count settings.

Defaults None.

Examples

```
> show advanced eap

EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries..... 20
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 1
EAP-Request Max Retries..... 20
EAPOL-Key Timeout (seconds)..... 1
EAPOL-Key Max Retries..... 2
```

Related Commands

- [Configure Advanced 802.11 Commands](#)
- [Show Advanced 802.11 Commands](#)

show advanced max-1x-sessions

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

show advanced max-1x-sessions

Syntax Description

show	Display settings.
advanced	Advanced configuration settings.
max-1x-sessions	Maximum number of simultaneous 802.1x sessions allowed per access point.

Defaults

None.

Examples

```
> show advanced max-1x-sessions
```

```
Max 802.1x session per AP at a given time..... 0
```

Related Commands

[Configure Advanced 802.11 Commands](#)
[Show Advanced 802.11 Commands](#)

show advanced probe

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

show advanced probe

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	probe	Number of probes sent to the WLAN controller per access point per client and the probe interval in milliseconds.

Defaults	None.

Examples To display the probe settings for the WLAN controller, enter this command:

```
> show advanced probe

Probe request filtering..... Enabled
Probes fwd to controller per client per radio.... 12
Probe request rate-limiting interval..... 100 msec
```

Related Commands	Configure Advanced 802.11 Commands Show Advanced 802.11 Commands

show advanced rate

To display whether control path rate limiting is enabled or disabled, use the **show advanced rate** command.

show advanced rate

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	rate	Control path rate limiting enabled or disabled.

Defaults

None.

Examples

```
> show advanced rate

Control Path Rate Limiting..... Disabled
```

Related Commands

[Configure Advanced 802.11 Commands](#)
[Show Advanced 802.11 Commands](#)

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	show	Display settings.
	advanced	Advanced configuration settings.
	send-disassoc-on-handoff	WLAN controller disassociates clients after a handoff enabled or disabled.

Defaults	None.

Examples	<pre>> show advanced send-disassoc-on-handoff Send Disassociate on Handoff..... Disabled</pre>

Related Commands	Configure Advanced 802.11 Commands Show Advanced 802.11 Commands

show advanced statistics

To display whether or not the Cisco Wireless LAN controller port statistics are enabled or disabled, use the **show advanced statistics** command.

show advanced statistics

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	statistics	Show configuration state of port statistics reporting.

Defaults

None.

Examples

```
> show advanced statistics

Switch port statistics..... Enabled
```

Related Commands

[Configure Advanced 802.11 Commands](#)
[Show Advanced 802.11 Commands](#)

show advanced timers

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

show advanced timers

Syntax Description	show	Display settings.
	advanced	Advanced configuration settings.
	timer	System timers.

Defaults Shown below in examples.

Examples

> **show advanced timers**

```
Authentication Response Timeout (seconds)..... 10
Rogue Entry Timeout (seconds)..... 1200
AP Heart Beat Timeout (seconds)..... 30
AP Discovery Timeout (seconds)..... 10
AP Local mode Fast Heartbeat (seconds)..... disable
AP Hreap mode Fast Heartbeat (seconds)..... disable
AP Primary Discovery Timeout (seconds)..... 120
```

Related Commands [Configure Advanced 802.11 Commands](#)
[Show Advanced 802.11 Commands](#)

Show Access Point Commands

Use the **show ap** commands to show access point settings.

show ap auto-rf

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

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

Syntax Description	show	Display settings.
	ap auto-rf	Cisco radio.
	802.11{a b}	802.11a or 802.11b/g setting.
	cisco_ap	Cisco lightweight access point name.

Defaults None.

Examples

> **show ap auto-rf 802.11a AP1**

```

Number Of Slots..... 2
AP Name..... AP03
MAC Address..... 00:0b:85:01:18:b7
Radio Type..... RADIO_TYPE_80211a
Noise Information
  Noise Profile..... PASSED
  Channel 36..... -88 dBm
  Channel 40..... -86 dBm
  Channel 44..... -87 dBm
  Channel 48..... -85 dBm
  Channel 52..... -84 dBm
  Channel 56..... -83 dBm
  Channel 60..... -84 dBm
  Channel 64..... -85 dBm
Interference Information
  Interference Profile..... PASSED
  Channel 36..... -66 dBm @ 1% busy
  Channel 40..... -128 dBm @ 0% busy
  Channel 44..... -128 dBm @ 0% busy
  Channel 48..... -128 dBm @ 0% busy
  Channel 52..... -128 dBm @ 0% busy
  Channel 56..... -73 dBm @ 1% busy
  Channel 60..... -55 dBm @ 1% busy
  Channel 64..... -69 dBm @ 1% busy
Rogue Histogram (20/40_ABOVE/40_BELOW)
  Channel 36..... 16/ 0/ 0
  Channel 40..... 28/ 0/ 0
  Channel 44..... 9/ 0/ 0
  Channel 48..... 9/ 0/ 0
  Channel 52..... 3/ 0/ 0
  Channel 56..... 4/ 0/ 0
  Channel 60..... 7/ 1/ 0
  Channel 64..... 2/ 0/ 0
Load Information
  Load Profile..... PASSED
  Receive Utilization..... 0%
  Transmit Utilization..... 0%
  Channel Utilization..... 1%
  Attached Clients..... 1 clients

```

```

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

```

Related Commands[Configure Access Point Commands](#)[Show Access Point Commands](#)

show ap ccx rm

To display an access point’s CCX radio management status information, use the **show ap ccx rm** command.

```
show ap ccx rm ap_name status
```

Syntax Description	show	Display settings.
	ap	Cisco lightweight access point settings.
	ccx	Cisco Client Extensions settings.
	rm	CCX radio management settings.
	ap_name	Specified access point name.
	status	Display CCX radio management status information for an access point.

Defaults
None.

```
Examples
> show ap ccx rm AP1240-21ac status

A Radio
  Channel Load Request ..... Disabled
  Noise Histogram Request ..... Disabled
  Beacon Request ..... Disabled
  Frame Request ..... Disabled
  Interval ..... 60
  Iteration ..... 10

G Radio
  Channel Load Request ..... Disabled
  Noise Histogram Request ..... Disabled
  Beacon Request ..... Disabled
  Frame Request ..... Disabled
  Interval ..... 60
  Iteration ..... 10
```

Related Commands

- [Configure Access Point Commands](#)
- [Show Access Point Commands](#)

show ap cdp

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

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

Syntax Description

show	Display settings.
ap	Cisco lightweight access point settings.
cdp	Cisco Discovery Protocol settings.
all ap-name neighbors	- Enter cdp all to display CDP status on all access points. - Enter cdp ap-name to display CDP status for a specified access point. - Enter cdp neighbors to display neighbors using CDP.
<i>ap_name</i>	Specified access point name.
all ap-name detail	- Enter neighbors all to show neighbors for all access points using CDP. - Enter neighbors ap-name to show neighbors for a specific access point using CDP. - Enter neighbors detail to display details about a specific access point neighbor using CDP.

Examples

> **show ap cdp all**

```
AP CDP State
AP Name          AP CDP State
-----
SB_RAP1          enable
SB_MAP1          enable
SB_MAP2          enable
SB_MAP3          enable
```

> **show ap cdp ap-name SB_RAP1**

```
AP CDP State
AP Name          AP CDP State
-----
SB_RAP1          enable
```

> **show ap cdp neighbors all**

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

```
> show ap cdp neighbors ap-name SB_MAP2
```

AP Name	AP IP	Neighbor Name	Neighbor IP	Neighbor Port
SB_MAP2	192.168.102.138	SB_MAP1	192.168.102.137	Virtual-Dot11Radio1
SB_MAP2	192.168.102.138	SB_MAP3	192.168.102.139	Virtual-Dot11Radio0

```
> show ap cdp neighbors detail SB_MAP2
```

```
AP Name:SB_MAP2
AP IP address:192.168.102.138
-----
Device ID: SB_MAP1
Entry address(es): 192.168.102.137
Platform: cisco AIR-LAP1522AG-A-K9 , Cap
Interface:Virtual-Dot11Radio0, Port ID (outgoingport):Virtual-Dot11Radio1
Holdtime : 180 sec

Version :
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Experimental Version 12.4(200
81114:084420) [BLD-v124_18a_ja_throttle.20081114 208] Copyright (c) 1986-2008 by
Cisco Systems, Inc. Compiled Fri 14-Nov-08 23:08 by

advertisement version: 2

-----
Device ID: SB_MAP3
Entry address(es): 192.168.102.139
Platform: cisco AIR-LAP1522AG-A-K9 , Capabilities: Trans-Bridge
Interface: Virtual-Dot11Radio1, Port ID (outgoing port): Virtual-Dot11Radio0
Holdtime : 180 sec

Version :
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Experimental Version 12.4(200
81114:084420) [BLD-v124_18a_ja_throttle.20081114 208] Copyright (c) 1986-2008 by
Cisco Systems, Inc. Compiled Fri 14-Nov-08 23:08 by

advertisement version: 2
```

Related Commands

[config ap cdp](#)
[config cdp timer](#)

show ap channel

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

show ap channel *ap_name*

Syntax Description	show	Display settings.
	ap	Display access point settings.
	channel	Display radio channel settings.
	<i>ap_name</i>	Name of mesh access point.

Examples

To view the available channels for access point *AP47*, enter this command:

```
>show ap channel AP47

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

Related Commands

[config 802.11-a channel ap](#)
[config 802.11h channelswitch](#)
[config 802.11h setchannel](#)

show ap config

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

show ap config {802.11{a | b} | general} cisco_ap

Syntax Description	show	Display settings.
	ap	Display access point settings.
	config	Display access point configuration settings.
	802.11	Display 802.11 radio settings.
	a b	Specifies 802.11a or 802.11b/g network.
	general	Displays general access point settings.
	<i>cisco_ap</i>	Specifies the lightweight access point name.

Defaults

None.

Examples

> **show ap config 802.11a AP02**

```

Cisco AP Identifier..... 0
Cisco AP Name..... AP02
AP Regulatory Domain..... Unconfigured
Switch Port Number ..... 1
MAC Address..... 00:0b:85:18:b6:50
IP Address Configuration..... DHCP
IP Address..... 1.100.49.240
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 1.100.49.1
Cisco AP Location..... default-location
Cisco AP Group Name..... default-group
Primary Cisco Switch..... Cisco_32:ab:63
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Sniffer
Public Safety ..... Global: Disabled, Local: Disabled
Sniffing ..... No
Remote AP Debug ..... Disabled
S/W Version ..... 3.1.61.0
Boot Version ..... 1.2.59.6
Stats Re--More-- or (q)uit
porting Period ..... 180
LED State..... Enabled
ILP Pre Standard Switch..... Disabled
ILP Power Injector..... Disabled
Number Of Slots..... 2
AP Model..... AS-1200
AP Serial Number..... 044110223A
AP Certificate Type..... Manufacture Installed

Attributes for Slot 0

```



```

Radio Type..... RADIO_TYPE_80211a
Administrative State ..... ADMIN_ENABLED
Operation State ..... UP
CellId ..... 0

Station Configuration
Configuration ..... AUTOMATIC
Number Of WLANs ..... 1
Medium Occupancy Limit ..... 100
CFP Period ..... 4
CFP MaxDuration ..... 60
BSSID ..... 00:0b:85:18:b6:50
Operation Rate Set
  6000 Kilo Bits..... MANDATORY
  9000 Kilo Bits..... SUPPORTED
  12000 Kilo Bits..... MANDATORY
  18000 Kilo Bits..... SUPPORTED
  24000 Kilo Bits..... MANDATORY
  36000 Kilo Bits..... SUPPORTED
  48000 Kilo Bits..... SUPPORTED
  54000 Kilo Bits..... SUPPORTED
Beacon Period ..... 100
DTIM Period ..... 1
Fragmentation Threshold ..... 2346
Multi Domain Capability Implemented ..... TRUE
Multi Domain Capability Enabled ..... TRUE
Country String ..... US

Multi Domain Capability
Configuration ..... AUTOMATIC
First Chan Num ..... 36
Number Of Channels ..... 4

MAC Operation Parameters
Configuration ..... AUTOMATIC
RTS Threshold ..... 2347
Short Retry Limit ..... 7
Long Retry Limit ..... 4
Fragmentation Threshold ..... 2346
Maximum Tx MSDU Life Time ..... 512
Maximum Rx Life Time ..... 512

Tx Power
Num Of Supported Power Levels ..... 5
Tx Power Level 1 ..... 18 dBm
Tx Power Level 2 ..... 15 dBm
Tx Power Level 3..... 12 dBm
Tx Power Level 4 ..... 9 dBm
Tx Power Level 5 ..... 6 dBm
Tx Power Configuration ..... CUSTOMIZED
Current Tx Power Level..... 5

Phy OFDM parameters
Configuration ..... AUTOMATIC
Current Channel ..... 36
TI Threshold ..... -50
Legacy Tx Beamforming Configuration ..... CUSTOMIZED
Legacy Tx Beamforming ..... ENABLED
Antenna Type..... INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBm units).... 11
AntennaMode..... ANTENNA_OMNI

Performance Profile Parameters
Configuration ..... AUTOMATIC

```

```

Interference threshold..... 10%
Noise threshold..... -70 dBm
RF utilization threshold..... 80%
Data-rate threshold..... 1000000 bps
Client threshold..... 12 clients
Coverage SNR threshold..... 16 dB
Coverage exception level..... 25%
Client minimum exception level..... 3 clients
Rogue Containment Information
Containment Count..... 0

```

> **show ap config 802.11b AP02**

```

Cisco AP Identifier..... 0
Cisco AP Name..... AP02
AP Regulatory Domain..... Unconfigured
Switch Port Number ..... 1
MAC Address..... 00:0b:85:18:b6:50
IP Address Configuration..... DHCP
IP Address..... 1.100.49.240
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 1.100.49.1
Cisco AP Location..... default-location
Cisco AP Group Name..... default-group
Primary Cisco Switch..... Cisco_32:ab:63
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Remote AP Debug ..... Disabled
S/W Version ..... 3.1.61.0
Boot Version ..... 1.2.59.6
Stats Reporting Period ..... 180
LED State..... Enabled
ILP Pre Standard Switch..... Disabled
ILP Power Injector..... Disabled
Number Of Slots..... 2
AP Model..... AS-1200
AP Serial Number..... 044110223A
AP Certificate Type..... Manufacture Installed

Attributes for Slot 1
Radio Type..... RADIO_TYPE_80211g
Administrative State ..... ADMIN_ENABLED
Operation State ..... UP
CellId ..... 0

Station Configuration
Configuration ..... AUTOMATIC
Number Of WLANs ..... 1
Medium Occupancy Limit ..... 100
CFP Period ..... 4
CFP MaxDuration ..... 60
BSSID ..... 00:0b:85:18:b6:50
Operation Rate Set
1000 Kilo Bits..... MANDATORY
2000 Kilo Bits..... MANDATORY
5500 Kilo Bits..... MANDATORY
11000 Kilo Bits..... MANDATORY
6000 Kilo Bits..... SUPPORTED
9000 Kilo Bits..... SUPPORTED
12000 Kilo Bits..... SUPPORTED

```

```

18000 Kilo Bits..... SUPPORTED
24000 Kilo Bits..... SUPPORTED
36000 Kilo Bits..... SUPPORTED
48000 Kilo Bits..... SUPPORTED
54000 Kilo Bits..... SUPPORTED
Beacon Period ..... 100
DTIM Period ..... 1
Fragmentation Threshold ..... 2346
Multi Domain Capability Implemented ..... TRUE
Multi Domain Capability Enabled ..... TRUE
Country String ..... US

Multi Domain Capability
Configuration ..... AUTOMATIC
First Chan Num ..... 1
Number Of Channels ..... 11

MAC Operation Parameters
Configuration ..... AUTOMATIC
RTS Threshold ..... 2347
Short Retry Limit ..... 7
Long Retry Limit ..... 4
Fragmentation Threshold ..... 2346
Maximum Tx MSDU Life Time ..... 512
Maximum Rx Life Time..... 512

Tx Power
Num Of Supported Power Levels..... 5
Tx Power Level 1 ..... 17 dBm
Tx Power Level 2..... 14 dBm
Tx Power Level 3..... 11 dBm
Tx Power Level 4..... 8 dBm
Tx Power Level 5..... 5 dBm
Tx Power Configuration..... CUSTOMIZED
Current Tx Power Level..... 5

Phy OFDM parameters
Configuration..... CUSTOMIZED
Current Channel..... 1
TI Threshold..... -50
Legacy Tx Beamforming Configuration ..... CUSTOMIZED
Legacy Tx Beamforming ..... ENABLED
Antenna Type..... INTERNAL_ANTENNA
Internal Antenna Gain (in5 dBm units)..... 11
Diversity..... DIVERSITY_ENABLED

Performance Profile Parameters
Configuration..... AUTOMATIC
Interference threshold..... 10%
Noise threshold..... -70 dBm
RF utilization threshold..... 80%
Data-rate threshold..... 1000000 bps
Client threshold..... 12 clients
Coverage SNR threshold..... 12 dB
Coverage exception level..... 25%
Client minimum exception level..... 3 clients
Rogue Containment Information
Containment Count..... 0

> show ap config general cisco-ap

Cisco AP Identifier..... 9
Cisco AP Name..... cisco-ap
Country code..... US - United States

```

```

Regulatory Domain allowed by Country..... 802.11bg:-A 802.11a:-A
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-A
Switch Port Number ..... 1
MAC Address..... 12:12:12:12:12:12
IP Address Configuration..... DHCP
IP Address..... 10.10.10.21
IP NetMask..... 255.255.255.0
CAPWAP Path MTU..... 1485
Domain.....
Name Server.....
Telnet State..... Disabled
Ssh State..... Disabled
Cisco AP Location..... default location
Cisco AP Group Name..... default-group
Primary Cisco Switch Name..... 4404
Primary Cisco Switch IP Address..... 10.10.10.32
Secondary Cisco Switch Name.....
Secondary Cisco Switch IP Address..... Not Configured
Tertiary Cisco Switch Name..... 4404
Tertiary Cisco Switch IP Address..... 3.3.3.3
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Public Safety ..... Global: Disabled, Local: Disabled
AP subMode ..... WIPS
Remote AP Debug ..... Disabled
S/W Version ..... 5.1.0.0
Boot Version ..... 12.4.10.0
Mini IOS Version ..... 0.0.0.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Enabled
PoE Power Injector MAC Addr..... Disabled
Power Type/Mode..... PoE/Low Power (degraded mode)
Number Of Slots..... 2
AP Model..... AIR-LAP1252AG-A-K9
IOS Version..... 12.4(10:0)
Reset Button..... Enabled
AP Serial Number..... serial_number
AP Certificate Type..... Manufacture Installed
Management Frame Protection Validation..... Enabled (Global MFP Disabled)
AP User Mode..... CUSTOMIZED
AP User Name..... maria
AP Dot1x User Mode..... Not Configured
AP Dot1x User Name..... Not Configured
Cisco AP system logging host..... 255.255.255.255
AP Up Time..... 4 days, 06 h 17 m 22 s
AP LWAPP Up Time..... 4 days, 06 h 15 m 00 s
Join Date and Time..... Mon Mar 3 06:19:47 2008

Ethernet Port Duplex..... Auto
Ethernet Port Speed..... Auto
AP Link Latency..... Enabled
Current Delay..... 0 ms
Maximum Delay..... 240 ms
Minimum Delay..... 0 ms
Last updated (based on AP Up Time)..... 4 days, 06 h 17 m 20 s

```

Related Commands

[Configure Access Point Commands](#)
[Show Access Point Commands](#)

show ap config global

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

show ap config global

Syntax Description	show	Display settings.
	ap	Display access point settings.
	config	Display Cisco radio configurations.
	global	Display global syslog server settings for all access points that join the controller.

Defaults	None.

Examples	<pre>> show ap config global AP global system logging host..... 255.255.255.255</pre>

Related Commands	Configure Access Point Commands Show Access Point Commands

show ap core-dump

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

```
show ap core-dump cisco_ap
```

Syntax Description

show	Display settings.
ap	Display access point settings.
core-dump	Display memory core dump information for a specified access point.
<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults

None.

Examples

```
> show ap core-dump AP02
```

Related Commands

[Configure Access Point Commands](#)
[Show Access Point Commands](#)

show ap crash-file

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

show ap crash-file

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	> show ap crash-file

Related Commands	Configure Access Point Commands Show Access Point Commands

show ap data-plane

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

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

Syntax Description

show	Display settings.
ap	Display access point settings.
data-plane	Display memory core dump information for a specified access point.
all	All Cisco lightweight access points.
<i>Cisco_AP</i>	Cisco lightweight access point name.

Defaults

None.

Examples

> **show ap data-plane all**

AP Name	Min Data Round Trip	Data Round Trip	Max Data Round Trip	Last Update
-----	-----	-----	-----	-----
1130	0.000s	0.000s	0.002s	18:51:23
1240	0.000s	0.000s	0.000s	18:50:45

Related Commands

[Configure Access Point Commands](#)
[Show Access Point Commands](#)

show ap eventlog

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

```
show ap eventlog ap_name
```

Syntax Description	ap_name	Displays the event log for the specified access point.

Defaults	None

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

Related Commands	Configure Access Point Commands Show Access Point Commands

show ap inventory

This command is used to display inventory information for an access point.

show ap inventory *ap_name*

Syntax Description

<i>ap_name</i>	Displays the inventory for the specified access point.

Defaults

None.

Examples

```
> show ap inventory test101
```

```
NAME: "test101"      , DESCR: "Cisco Wireless Access Point"  
PID: AIR-LAP1131AG-A-K9  , VID: V01,  SN: FTX1123T2XX
```

Related Commands

[Configure Access Point Commands](#)
[Show Access Point Commands](#)

show ap join stats detail

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

show ap join stats detail *ap_mac*

Syntax Description

show	Display settings.
ap	All Cisco lightweight access points.
join stats detail	Join-related statistics collected for a specific access point.
<i>ap_mac</i>	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.

Examples

```
> show ap join stats detail 00:0b:85:02:0d:20
Discovery phase statistics
- Discovery requests received..... 2
- Successful discovery responses sent..... 2
- Unsuccessful discovery request processing..... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt..... Aug 21 12:50:23:335
- Time at last unsuccessful discovery attempt..... Not applicable

Join phase statistics
- Join requests received..... 1
- Successful join responses sent..... 1
- Unsuccessful join request processing..... 1
- Reason for last unsuccessful join attempt.....RADIUS authorization is pending
for the AP
- Time at last successful join attempt..... Aug 21 12:50:34:481
- Time at last unsuccessful join attempt..... Aug 21 12:50:34:374

Configuration phase statistics
- Configuration requests received..... 1
- Successful configuration responses sent..... 1
- Unsuccessful configuration request processing..... 0
- Reason for last unsuccessful configuration attempt... Not applicable
- Time at last successful configuration attempt..... Aug 21 12:50:34:374
- Time at last unsuccessful configuration attempt..... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure..... Not applicable

Last AP disconnect details
- Reason for last AP connection failure..... Not applicable

Last join error summary
- Type of error that occurred last..... Lwapp join request rejected
- Reason for error that occurred last..... RADIUS authorization is pending
for the AP
- Time at which the last join error occurred..... Aug 21 12:50:34:374
```

Related Commands

[Configure Access Point Commands](#)
[Show Access Point Commands](#)

show ap join stats summary

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

show ap join stats summary *ap_mac*

Syntax Description	show	Display settings.
	ap	All Cisco lightweight access points.
	join stats summary	Summary of all access points that joined or attempted to join to the controller.
	<i>ap_mac</i>	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.



Usage Guidelines	Note	To obtain the MAC address of the 802.11 radio interface, enter the show interface command on the access point.

Examples

```
> show ap join stats summary 00:0b:85:02:0d:20
```

```
Is the AP currently connected to controller..... No
Time at which the AP joined this controller last time..... Aug 21 12:50:36:061
Type of error that occurred last..... Lwapp join request
rejected
Reason for error that occurred last..... RADIUS authorization
is pending for the AP
Time at which the last join error occurred..... Aug 21 12:50:34:374
```

Related Commands

[Configure Access Point Commands](#)
[Show Access Point Commands](#)
[show interface](#)

show ap join stats summary all

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

show ap join stats summary all

Syntax Description

show	Display settings.
ap	All Cisco lightweight access points.
join stats summary	Summary of all access points that joined or attempted to join to the controller.

Defaults

None.

Examples

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

Related Commands

[Configure Access Point Commands](#)
[Show Access Point Commands](#)

show ap link-encryption

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

show ap link-encryption {all | Cisco_AP}

Syntax Description

show	Display settings.
ap	Access point settings.
link-encryption	Link encryption status for an access point.
all Cisco_AP	Cisco lightweight access point or all access points.

Defaults

None.

Examples

> **show ap link-encryption all**

AP Name	Encryption State	Dnstream Count	Upstream Count	Last Update
1240	Dis	4406	237553	Never
1130	En	2484	276308	19:31

Related Commands

[Configure Access Point Commands](#)
[Show Access Point Commands](#)

show ap monitor-mode summary

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

show ap monitor-mode summary

Syntax Description	show	Display settings.
	ap	Access point settings.
	monitor-mode	Channel-optimized monitor mode settings.
	summary	Display all settings.

Defaults None.

Examples To display current channel-optimized monitor mode settings, enter this command:

> **show ap monitor-mode summary**

AP Name	Ethernet MAC	Status	Scanning Channel List
-----	-----	-----	-----
AP_004	xx:xx:xx:xx:xx:xx	Tracking	1, 6, 11, 4

Related Commands [Configure Access Point Commands](#)
[Show Access Point Commands](#)

show ap stats

To display the statistics for a Cisco lightweight access point, use the **show ap stats** command.

show ap stats { **802.11**{ **a** | **b** } | **wlan** } *cisco_ap*

Syntax Description	show	Display settings.
	ap stats	Cisco radio.
	802.11	Display the access point's 802.11 radio statistics.
	a b	Specifies 802.11a or 802.11b/g network.
	wlan	WLAN statistics.
	<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults None.

Examples

> **show ap stats 802.11b AP02**

```

Number Of Slots..... 2
AP Name..... AP02
MAC Address..... 00:0b:85:18:b6:50
  Radio Type..... RADIO_TYPE_80211a
  Stats Information
    Number of Users..... 0
    TxFragmentCount..... 1679
    MulticastTxFrameCnt..... 1260
    FailedCount..... 15892
    RetryCount..... 331
    MultipleRetryCount..... 0
    FrameDuplicateCount..... 0
    RtsSuccessCount..... 0
    RtsFailureCount..... 0
    AckFailureCount..... 80212
    RxFragmentCount..... 248671
    MulticastRxFrameCnt..... 0
    FcsErrorCount..... 105968
    TxFrameCount..... 1679
    WepUndecryptableCount..... 0

```

Related Commands [Configure Access Point Commands](#)
[Show Access Point Commands](#)

show ap summary

To display a summary of all lightweight access points attached to the controller, use the **show ap summary** command. A list containing each lightweight access point name, number of slots, manufacturer, MAC address, location and the controller port number is displayed.

show ap summary

Syntax Description	show	Display settings.
	ap	All Cisco lightweight access points.
	summary	Summary of all Cisco lightweight access points.

Defaults	None.

Examples

```
> show ap summary
Number of APs..... 2
Global AP User Name..... user
Global AP Dot1x User Name..... Not Configured

Number of APs..... 2
Global AP User Name..... user
Global AP Dot1x User Name..... Not Configured

AP Name    Slots  AP Model          Ethernet MAC      Location    Port Country  Priority
-----
wolverine  2          AIR-LAP1252AG-A-K9  00:1b:d5:13:39:74 Reception  1    US         3
ap:1120    1          AIR-LAP1121G-A-K9  00:1b:d5:a9:ad:08 Hall 235   1    US         1
```

Related Commands	Configure Access Point Commands
	Show Access Point Commands

show ap tcp-mss-adjust

To display the BSSID value for each WLAN defined on an access point, use the **show ap wlan** command.

show ap tcp-mss-adjust {*cisco_ap* | **all**}

Syntax Description	show	Display settings.
	ap	All Cisco lightweight access points.
	tcp-mss-adjust	Wireless LAN parameter.
	<i>cisco_ap</i>	Specifies the lightweight access point name.
	all	All access points.

Defaults None.

Examples

> **show ap tcp-mss-adjust all**

```

AP Name          TCP State MSS Size
-----
AP-1140          enabled  536
AP-1240          disabled -
AP-1130          disabled -

```

Related Commands [config ap tcp-adjust-mss](#)

show ap wlan

To display the BSSID value for each WLAN defined on an access point, use the **show ap wlan** command.

show ap wlan 802.11{a | b} cisco_ap

Syntax Description

show	Display settings.
ap	All Cisco lightweight access points.
wlan	Wireless LAN parameter.
802.11	Display the access point's 802.11 radio statistics.
a b	Specifies 802.11a or 802.11b/g network.
<i>ap_name</i>	Specifies the lightweight access point name.

Defaults

None.

Examples

```
> show ap wlan 802.11b AP01
```

```
Site Name..... MY_AP_GROUP1
Site Description..... MY_AP_GROUP1
```

WLAN ID	Interface	BSSID
-----	-----	-----
1	management	00:1c:0f:81:fc:20
2	dynamic	00:1c:0f:81:fc:21

Related Commands

[Configure Access Point Commands](#)
[Show Access Point Commands](#)

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	show	Display settings.
	arp	Address Resolution Protocol (ARP) settings.
	switch	Cisco Wireless LAN controller settings.

Defaults	None.

Examples

```
> 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 auth-list

To display the access point authorization list, use the **show auth-list** command.

show auth-list

Syntax Description	show	Display settings.
	auth-list	Displays access point authorization list.

Defaults	None.

Examples	<pre>> show auth-list Authorize APs against AAA..... disabled Allow APs with Self-signed Certificate (SSC)... disabled Mac Addr Cert Type Key Hash ----- xx:xx:xx:xx:xx:xx MIC</pre>

Related Commands	clear radius auth statistics clear stats local-auth config auth-list add config auth-list ap-policy config auth-list delete

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

show	Display settings.
boot	Software bootable versions.

Usage Guidelines

Each Cisco Wireless LAN controller retains one primary and one backup operating system software load in non-volatile RAM. This allows operators to have the Cisco Wireless LAN controllers boot off the primary load (default), or revert to the backup load when desired.

Examples

```
> show boot
```

```
Primary Boot Image..... 3.2.13.0 (active)
Backup Boot Image..... 3.2.15.0
```

Related Commands

[config exclusionlist](#)
[show client detail](#)

show call-control ap

To see the metrics for successful calls or the traps generated for failed calls, use the **show call-control ap** command.

show call-control ap {802.11a | 802.11b} Cisco_AP {metrics | traps}

Syntax Description

show	Display settings.
call-control	Call control settings.
ap	Access point-related information.
802.11a 802.11b	Specifies type of 802.11 network.
<i>Cisco_AP</i>	Cisco access point name.
metrics	Call metrics information.
traps	Trap info for call control.

Defaults

None.

Examples

```
> show call-control ap 802.11a Cisco_AP metrics
Total Call Duration in Seconds..... 120
Number of Calls..... 10

Number of calls for given client is..... 1

> show call-control ap 802.11a Cisco_AP traps
Number of traps sent in one min..... 2
Last SIP error code..... 404
Last sent trap timestamp..... Jun 20 10:05:06
```

To aid in troubleshooting, the output of this command shows an error code for any failed calls. [Table 1-1](#) explains the possible error codes for failed calls.

Table 1-1 Error Codes for Failed VoIP Calls

Error Code	Integer	Description
1	unknown	Unknown error.
400	badRequest	The request could not be understood because of malformed syntax.
401	unauthorized	The request requires user authentication.
402	paymentRequired	Reserved for future use.
403	forbidden	The server understood the request but refuses to fulfill it.
404	notFound	The server has information that the user does not exist at the domain specified in the Request-URI.
405	methodNotAllowed	The method specified in the Request-Line is understood but not allowed for the address identified by the Request-URI.

Table 1-1 Error Codes for Failed VoIP Calls

Error Code	Integer	Description
406	notAcceptable	The resource identified by the request is only capable of generating response entities with content characteristics that are not acceptable according to the Accept header field sent in the request.
407	proxyAuthenticationRequired	The client must first authenticate with the proxy.
408	requestTimeout	The server could not produce a response within a suitable amount of time, if it could not determine the location of the user in time.
409	conflict	The request could not be completed due to a conflict with the current state of the resource.
410	gone	The requested resource is no longer available at the server, and no forwarding address is known.
411	lengthRequired	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
413	requestEntityTooLarge	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
414	requestURITooLarge	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415	unsupportedMediaType	The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method.
420	badExtension	The server did not understand the protocol extension specified in a Proxy-Require or Require header field.
480	temporarilyNotAvailable	The callee's end system was contacted successfully, but the callee is currently unavailable.
481	callLegDoesNotExist	The UAS received a request that does not match any existing dialog or transaction.
482	loopDetected	The server has detected a loop.
483	tooManyHops	The server received a request that contains a Max-Forwards header field with the value zero.
484	addressIncomplete	The server received a request with a Request-URI that was incomplete.
485	ambiguous	The Request-URI was ambiguous.
486	busy	The callee's end system was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system.
500	internalServerError	The server encountered an unexpected condition that prevented it from fulfilling the request.
501	notImplemented	The server does not support the functionality required to fulfill the request.

Table 1-1 **Error Codes for Failed VoIP Calls**

Error Code	Integer	Description
502	badGateway	The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
503	serviceUnavailable	The server is temporarily unable to process the request because of a temporary overloading or maintenance of the server.
504	serverTimeout	The server did not receive a timely response from an external server it accessed in attempting to process the request.
505	versionNotSupported	The server does not support or refuses to support the SIP protocol version that was used in the request.
600	busyEverywhere	The callee's end system was contacted successfully, but the callee is busy or does not want to take the call at this time.
603	decline	The callee's machine was contacted successfully, but the user does not want to or cannot participate.
604	doesNotExistAnywhere	The server has information that the user indicated in the Request-URI does not exist anywhere.
606	notAcceptable	The user's agent was contacted successfully, but some aspects of the session description (such as the requested media, bandwidth, or addressing style) were not acceptable.

Related Commands

[config wlan call-snoop](#)
[show call-control client](#)

show call-control client

To see call information for a call-aware client when VoIP snooping is enabled and the call is active, use the show call-control client command

show call-control client callInfo *client_MAC_address*

Syntax Description	show	Display settings.
	call-control	Call control settings.
	client	Client-related information.
	callInfo	Call-control information information.
	<i>client_MAC_address</i>	Client MAC address.

Defaults None.

Examples

```
> show call-control client callInfo 10.10.10.10.10
```

```
Uplink IP/port..... 10.10.1.71 / 23870
Downlonk IP/port..... 10.10.1.47 / 2070
UP..... 6
Calling Party..... sip:1054
Called Party..... sip:1000
Call ID..... 58635b00-850161b7-14853-1501a8
Number of calls for given client is..... 1
```

Related Commands

[config wlan call-snoop](#)

[show call-control ap](#)

show capwap reap association

To display the list of clients associated to an access point and their SSIDs, use the **show capwap reap association** command.

show capwap reap association

Syntax Description

show	Display settings.
capwap	Control and Provisioning of Wireless Access Points settings.
reap	Hybrid-REAP settings.
association	Display clients associated to this access point and their SSIDs.

Defaults

None.

Examples

```
> show capway reap association
```

Related Commands

[config hreap group](#)
[show capwap reap status](#)

show capwap reap status

To display the status of the hybrid-REAP access point (connected or standalone), use the **show capwap reap status** command.

show capwap reap status

Syntax Description	show	Display settings.
	capwap	Control and Provisioning of Wireless Access Points settings.
	reap	Hybrid-REAP settings.
	status	Display status of the hybrid-REAP access point.

Defaults None.

Examples > **show capwap reap status**

Related Commands [config hreap group](#)
[show capwap reap association](#)

show certificate compatibility

To display whether or not certificates are verified as compatible in the Cisco Wireless LAN controller, use the **show certificate compatibility** command.

show certificate compatibility

Syntax Description

show	Display settings.
certificate	All certificates.
compatibility	Compatibility of certificates.

Defaults

None.

Examples

```
> show certificate compatibility
```

```
Certificate compatibility mode:..... off
```

Related Commands

[config certificate](#)
[config certificate lsc](#)
[show certificate lsc](#)
[show certificate summary](#)
[show local-auth certificates](#)

show certificate lsc

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

show certificate lsc {summary | ap-provision}

Syntax Description	show	Display settings.
	certificate	Certificate settings.
	lsc	Locally Significant Certificate settings.
	summary	Display a summary of LSC certificate settings and certificates.
	ap-provision	Display details about the access points that are provisioned using LSC.

Defaults None.

Examples

> **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
```

> **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](#)
- [config certificate lsc](#)
- [show certificate compatibility](#)
- [show certificate summary](#)
- [show local-auth certificates](#)

show certificate summary

To verify that the controller has generated a certificate, use the **show certificate summary** command.

show certificate summary

Syntax Description	show	Display settings.
	certificate	All certificates.
	summary	Synopsis of all certificates.

Defaults	None.

Examples	<pre>> show certificate summary Web Administration Certificate..... Locally Generated Web Authentication Certificate..... Locally Generated Certificate compatibility mode:..... off</pre>

Related Commands	config certificate config certificate lsc show certificate compatibility show certificate lsc show local-auth certificates

Show Client Commands

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

show client ap

To display the clients on a Cisco lightweight access point, use the **show client ap** command.

```
show client ap 802.11{a | b} cisco_ap
```

Syntax Description

show	Display settings.
client	Client settings.
ap	Cisco lightweight access point settings.
802.11	802.11 network settings.
a b	- Enter a if the client access point resides on an 802.11a network. - Enter b if the client access point resides on an 802.11b network.
<i>cisco_ap</i>	Cisco lightweight access point name.

Usage Guidelines

The **show client ap** command may list the status of automatically disabled clients. Use the [show exclusionlist](#) command to view clients on the exclusion list (blacklisted).

Examples

```
> show client ap 802.11b AP1
```

MAC Address	AP Id	Status	WLAN Id	Authenticated
-----	-----	-----	-----	-----
xx:xx:xx:xx:xx:xx	1	Associated	1	No

Related Commands

[show client detail](#)
[show client summary](#)
[show client username](#)
[show exclusionlist](#)

show client ccx client-capability

To view the client's capability information, use the **show client ccx client-capability** command.

show client ccx client-capability *client_mac_address*

Syntax Description	show	Display settings.
	client	Client settings.
	ccx	Cisco Compatible Extensions (CCX) settings.
	client-capability	Display client capability information.
	<i>client_mac_address</i>	Specifies the MAC address of the client.

Defaults None.

Usage Guidelines This command displays the client's available capabilities, not current settings for the capabilities.

Examples

```
> show client ccx client-capability 00:40:96:a8:f7:98
Service Capability..... Voice, Streaming(uni-directional)
Video, Interactive(bi-directional) Video
Radio Type..... DSSS OFDM(802.11a) HRDSSS(802.11b)
ERP(802.11g)

Radio Type..... DSSS
  Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode..... Automatic
  Rate List(MB)..... 1.0 2.0

Radio Type..... HRDSSS(802.11b)
  Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode..... Automatic
  Rate List(MB)..... 5.5 11.0

Radio Type..... ERP(802.11g)
  Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode..... Automatic
  Rate List(MB)..... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Are you sure you want to start? (y/N)y Are you sure you want to start? (y/N)
```

Related Commands

- [config client ccx get-client-capability](#)
- [config client ccx get-operating-parameters](#)
- [config client ccx get-profiles](#)
- [config client ccx stats-request](#)
- [show client ccx operating-parameters](#)
- [show client ccx profiles](#)
- [show client ccx stats-report](#)

show client ccx frame-data

To view the data frames sent from the client for the last test, use the **show client ccx frame-data** command.

show client ccx frame-data *client_mac_address*

Syntax Description	show	Display settings.
	client	Client settings.
	ccx	Cisco Compatible Extensions (CCX) settings.
	frame-data	Display client CCX data frames.
	<i>client_mac_address</i>	Specifies the MAC address of the client.

Defaults None.

Examples

```
> LOG Frames:
Frame Number ..... 1
Last Frame Number ..... 1120
Direction ..... 1
Timestamp ..... 0d 00h 50m 39s 863954us
Frame Length ..... 197
Frame Data:
00000000: 80 00 00 00 ff ff ff ff ff 00 12 44 bd bd b0 .....D...
00000010: 00 12 44 bd bd b0 f0 af 43 70 00 f2 82 01 00 00 ..D....Cp.....
00000020: 64 00 11 08 00 01 00 01 08 8c 12 98 24 b0 48 60 d.....$.H'
00000030: 6c 05 04 01 02 00 00 85 1e 00 00 89 00 0f 00 ff 1.....
00000040: 03 19 00 41 50 32 33 2d 31 30 00 00 00 00 00 00 ...AP23-10.....
00000050: 00 00 00 00 00 00 26 96 06 00 40 96 00 ff ff dd .....&...@.....
00000060: 18 00 50 f2 01 01 00 00 50 f2 05 01 00 00 50 f2 ..P....P....P.
00000070: 05 01 00 00 40 96 00 28 00 dd 06 00 40 96 01 01 ....@..(....@...

00000080: 00 dd 05 00 40 96 03 04 dd 16 00 40 96 04 00 02 ....@.....@....
00000090: 07 a4 00 00 23 a4 00 00 42 43 00 00 62 32 00 00 ....#...BC..b2..
000000a0: dd 05 00 40 96 0b 01 dd 18 00 50 f2 02 01 01 82 ...@.....P.....
000000b0: 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 32 2f .....'....BC^.b2/

> LOG Frames:
Frame Number ..... 2
Last Frame Number ..... 1120
Direction ..... 1
Timestamp ..... 0d 00h 50m 39s 878289us
Frame Length ..... 147
Frame Data:
00000000: 80 00 00 00 ff ff ff ff ff 00 0d ed c3 a0 22 .....
00000010: 00 0d ed c3 a0 22 00 bd 4d 50 a5 f7 78 08 00 00 .....".MP..x...
00000020: 64 00 01 00 00 01 00 01 08 8c 12 98 24 b0 48 60 d.....$.H'
00000030: 6c 05 04 01 02 00 00 85 1e 00 00 84 00 0f 00 ff 1.....
00000040: 03 19 00 72 6f 67 75 65 2d 74 65 73 74 31 00 00 ...rogue-test1..
00000050: 00 00 00 00 00 00 23 96 06 00 40 96 00 10 00 dd .....#...@.....
00000060: 06 00 40 96 01 01 00 dd 05 00 40 96 03 04 dd 05 ....@.....@...
00000070: 00 40 96 0b 01 dd 18 00 50 f2 02 01 01 81 00 03 ....@.....@...
00000080: a4 00 00 27 a4 00 00 42 43 5e 00 62 32 2f 00 d2 ...'....BC^.b2/..
00000090: b4 ab 84
...
```

```

> LOG Frames:
Frame Number ..... 3
Last Frame Number ..... 1120
Direction ..... 1
Timestamp ..... 0d 00h 50m 39s 881513us
Frame Length ..... 189
Frame Data:
00000000: 80 00 00 00 ff ff ff ff ff ff 00 12 44 bd 80 30 .....D..0
00000010: 00 12 44 bd 80 30 60 f7 46 c0 8b 4b d1 05 00 00 ..D..0'.F..K...
00000020: 64 00 11 08 00 01 00 01 08 8c 12 98 24 b0 48 60 d.....$.H'
00000030: 6c 05 04 00 02 00 00 85 1e 00 00 89 00 0f 00 ff 1.....
00000040: 03 19 00 41 50 34 30 2d 31 37 00 00 00 00 00 00 ...AP23-10.....
00000050: 00 00 00 00 00 00 26 dd 18 00 50 f2 01 01 00 00 .....&...P.....
00000060: 50 f2 05 01 00 00 50 f2 05 01 00 00 40 96 00 28 P.....P.....@..(
00000070: 00 dd 06 00 40 96 01 01 00 dd 05 00 40 96 03 04 ....@.....@...

00000080: dd 16 00 40 96 04 00 05 07 a4 00 00 23 a4 00 00 ....@.....#. ....
00000090: 42 43 00 00 62 32 00 00 dd 05 00 40 96 0b 01 dd BC..b2.....@....
000000a0: 18 00 50 f2 02 01 01 85 00 03 a4 00 00 27 a4 00 ..P.....'...
000000b0: 00 42 43 5e 00 62 32 2f 00 0b 9a 1d 6f .....BC^.b2/.....o...

```

Related Commands [show client ccx last-response-status](#)

show client ccx last-response-status

To view the status of the last test response, use the **show client ccx last-response-status** command.

show client ccx last-response-status *client_mac_address*

Syntax Description	show	Display settings.
	client	Client settings.
	ccx	Cisco Compatible Extensions (CCX) settings.
	last-response-status	Display the status of the last CCX client test response.
	<i>client_mac_address</i>	Specifies the MAC address of the client.

Defaults None.

Examples

```
> show client ccx last-response-status
Test Status ..... Success

Response Dialog Token..... 87
Response Status..... Successful
Response Test Type..... 802.1x Authentication Test
Response Time..... 3476 seconds since system boot
```

Related Commands

- config client ccx default-gw-ping
- config client ccx dhcp
- config client ccx dns-ping
- config client ccx dns-resolve
- config client ccx test-association
- config client ccx test-dot1x
- config client ccx test-profile
- config client ccx test-abort
- config client ccx clear-results
- config client ccx send-message
- show client ccx last-response-status
- show client ccx results
- show client ccx frame-data

show client ccx last-test-status

To view the status of the last test, use the **show client ccx last-test-status** command.

show client ccx last-test-status *client_mac_address*

Syntax Description	show	Display settings.
	client	Client settings.
	ccx	Cisco Compatible Extensions (CCX) settings.
	last-test-status	Display the status of the last CCX client test.
	<i>client_mac_address</i>	Specifies the MAC address of the client.

Defaults None.

Examples

```
> show client ccx last-test-status

Test Type ..... Gateway Ping Test
Test Status ..... Pending/Success/Timeout
Dialog Token ..... 15
Timeout ..... 15000 ms
Request Time ..... 1329 seconds since system boot
```

Related Commands

- config client ccx default-gw-ping
- config client ccx dhcp
- config client ccx dns-ping
- config client ccx dns-resolve
- config client ccx test-association
- config client ccx test-dot1x
- config client ccx test-profile
- config client ccx test-abort
- config client ccx clear-results
- config client ccx send-message
- show client ccx last-response-status
- show client ccx results
- show client ccx frame-data

show client ccx log-response

To display a log response, use the **show client ccx log-response** command.

show client ccx log-response [**roam** | **rsna** | **syslog**] *client_mac_address*

Syntax Description		
show		Display settings.
client		Client settings.
ccx		Cisco Compatible Extensions (CCX) settings.
log-response		Display a CCX client log response.
roam		Displays CCX client roaming log response.
rsna		Displays CCX client RSNA log response.
syslog		Displays CCX client system log response.
<i>client_mac_address</i>		Displays the inventory for the specified access point.

Defaults None.

Examples

```
> config client ccx log-request syslog 00:40:96:a8:f7:98
> show client ccx log-response syslog 00:40:96:a8:f7:98
Tue Jun 26 18:07:48 2007 Syslog Response LogID=131: Status=Successful
                        Event Timestamp=0d 00h 19m 42s 278987us
                        Client SysLog = '<11> Jun 19 11:49:47 unraval13777 Mandatory
elements missing in the OID response'
                        Event Timestamp=0d 00h 19m 42s 278990us
                        Client SysLog = '<11> Jun 19 11:49:47 unraval13777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007 Syslog Response LogID=131: Status=Successful
                        Event Timestamp=0d 00h 19m 42s 278987us
                        Client SysLog = '<11> Jun 19 11:49:47 unraval13777 Mandatory
elements missing in the OID response'
                        Event Timestamp=0d 00h 19m 42s 278990us
                        Client SysLog = '<11> Jun 19 11:49:47 unraval13777 Mandatory
elements missing in the OID response'

> config client ccx log-request roam 00:40:96:a8:f7:98
> show client ccx log-response roam 00:40:96:a8:f7:98

Thu Jun 22 11:55:14 2007 Roaming Response LogID=20: Status=Successful
                        Event Timestamp=0d 00h 00m 13s 322396us
                        Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
                        Transition Time=100(ms)
                        Transition Reason: Normal roam, poor link
                        Transition Result: Success
Thu Jun 22 11:55:14 2007 Roaming Response LogID=133: Status=Successful
                        Event Timestamp=0d 00h 00m 16s 599006us
                        Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2,
                        Transition Time=3235(ms)
                        Transition Reason: Normal roam, poor link
                        Transition Result: Success
Thu Jun 22 18:28:48 2007 Roaming Response LogID=133: Status=Successful
                        Event Timestamp=0d 00h 00m 08s 815477us
```

```

Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:d2,
Transition Time=3281(ms)
Transition Reason: First association to WLAN
Transition Result: Success

```

```

> config client ccx log-request rsna 00:40:96:a8:f7:98
> show client ccx log-response rsna 00:40:96:a8:f7:98

```

```

Tue Oct 05 11:06:48 2006
  RSNA Response LogID=2: Status=Successful
  Event Timestamp=242424242424
  Target BSSID=00:0b:85:23:26:70
  RSNA Version=1
  Group Cipher Suite=00-0f-ac-01
  Pairwise Cipher Suite Count = 2
    Pairwise Cipher Suite 0 = 00-0f-ac-02
    Pairwise Cipher Suite 1 = 00-0f-ac-04
  AKM Suite Count = 2
    KM Suite 0 = 00-0f-ac-01
    KM Suite 1 = 00-0f-ac-02
  SN Capability = 0x1
  PMKID Count = 2
    PMKID 0 = 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
    PMKID 1 = 0a 0b 0c 0d 0e 0f 17 18 19 20 1a 1b 1c 1d 1e 1f
  802.11i Auth Type: EAP_FAST
  RSNA Result: Success
Tue Oct 05 11:05:48 2006
  RSNA Request LogID=2

```

Related Commands [config client ccx log-request](#)

show client ccx manufacturer-info

To view the client manufacturing information, use the **show client ccx manufacturer-info** command.

show client ccx manufacturer-info *client_mac_address*

Syntax Description		
show		Display settings.
client		Client settings.
ccx		Cisco Compatible Extensions (CCX) settings.
manufacturer-info		Display CCX client technical specifications.
<i>client_mac_address</i>		Specifies the MAC address of the client.

Examples

```
> show client ccx manufacturer-info 00:40:96:a8:f7:98
Manufacturer OUI ..... 00:40:96
Manufacturer ID ..... Cisco
Manufacturer Model ..... Cisco Aironet 802.11a/b/g Wireless Adapter
Manufacturer Serial ..... FOC1046N3SX
Mac Address ..... 00:40:96:b2:8d:5e
Radio Type ..... DSSS OFDM(802.11a) HRDSSS(802.11b)
ERP(802.11g)
Antenna Type ..... Omni-directional diversity
Antenna Gain ..... 2 dBi

Rx Sensitivity:
Radio Type ..... DSSS
Rx Sensitivity ..... Rate:1.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ..... Rate:2.0 Mbps, MinRssi:-95, MaxRssi:-30
Radio Type ..... HRDSSS(802.11b)
Rx Sensitivity ..... Rate:5.5 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ..... Rate:11.0 Mbps, MinRssi:-95, MaxRssi:-30
Radio Type ..... ERP(802.11g)
Rx Sensitivity ..... Rate:6.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ..... Rate:9.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ..... Rate:12.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ..... Rate:18.0 Mbps, MinRssi:-95, MaxRssi:-30
```

Related Commands

```
config client ccx get-profiles
config client ccx get-operating-parameters
config client ccx get-manufacturer-info
config client ccx get-client-capability
show client ccx profiles
show client ccx operating-parameters
show client ccx client-capability
config client ccx stats-request
show client ccx stats-report
```

show client ccx operating-parameters

To view the client operating-parameters, use the **show client ccx operating-parameters** command.

show client ccx operating-parameters *client_mac_address*

Syntax Description	show	Display settings.
	client	Client settings.
	ccx	Cisco Compatible Extensions (CCX) settings.
	operating-parameters	Display a CCX client configuration settings.
	<i>client_mac_address</i>	Specifies the MAC address of the client.

Examples

> **show client ccx operating-parameters 00:40:96:a8:f7:98**

```
Client Mac ..... 00:40:96:b2:8d:5e
Radio Type ..... OFDM(802.11a)

Radio Type ..... OFDM(802.11a)
  Radio Channels ..... 36 40 44 48 52 56 60 64 100 104 108
112 116 120 124 128 132 136 140 149 153 157 161 165
  Tx Power Mode ..... Automatic
  Rate List(MB)..... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Power Save Mode ..... Normal Power Save
SSID ..... wifi
Security Parameters[EAP Method, Credential]..... None
Auth Method ..... None
Key Management..... None
Encryption ..... None
Device Name ..... Wireless Network Connection 15
Device Type ..... 0
OS Id ..... Windows XP
OS Version ..... 5.1.6.2600 Service Pack 2
IP Type ..... DHCP address
IPv4 Address ..... Available
IP Address ..... 70.0.4.66
Subnet Mask ..... 255.0.0.0
Default Gateway ..... 70.1.0.1
IPv6 Address ..... Not Available
IPv6 Address ..... 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
IPv6 Subnet Mask ..... 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
DNS Servers ..... 103.0.48.0
WINS Servers .....
System Name ..... URAVAL3777
Firmware Version ..... 4.0.0.187
Driver Version ..... 4.0.0.187
```

Related Commands

[config client ccx get-client-capability](#)
[config client ccx get-manufacturer-info](#)
[config client ccx get-operating-parameters](#)
[config client ccx get-profiles](#)

show client ccx profiles

To view the client profiles, use the **show client ccx profiles** command.

show client ccx profiles *client_mac_address*

Syntax	Description
show	Display settings.
client	Client settings.
ccx	Cisco Compatible Extensions (CCX) settings.
profiles	Display profiles for a CCX client.
<i>client_mac_address</i>	Specifies the MAC address of the client.

Examples

```
> show client ccx profiles 00:40:96:a8:f7:98
Number of Profiles ..... 1
Current Profile ..... 1

Profile ID ..... 1
Profile Name ..... wifiEAP
SSID ..... wifiEAP
Security Parameters [EAP Method, Credential]..... EAP-TLS, Host OS Login Credentials
Auth Method ..... EAP
Key Management ..... WPA2+CCKM
Encryption ..... AES-CCMP
Power Save Mode ..... Constantly Awake
Radio Configuration:
Radio Type..... DSSS
    Preamble Type..... Long preamble
    CCA Method..... Energy Detect + Carrier
Detect/Correlation
    Data Retries..... 6
    Fragment Threshold..... 2342
    Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
    Tx Power Mode..... Automatic
    Rate List (MB)..... 1.0 2.0

Radio Type..... HRDSSS(802.11b)
    Preamble Type..... Long preamble
    CCA Method..... Energy Detect + Carrier
Detect/Correlation
    Data Retries..... 6
    Fragment Threshold..... 2342
    Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
    Tx Power Mode..... Automatic
    Rate List (MB)..... 5.5 11.0

Radio Type..... ERP(802.11g)
    Preamble Type..... Long preamble
    CCA Method..... Energy Detect + Carrier
Detect/Correlation
    Data Retries..... 6
    Fragment Threshold..... 2342
    Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
    Tx Power Mode..... Automatic
    Rate List (MB)..... 6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0
```

```

Radio Type..... OFDM(802.11a)
  Preamble Type..... Long preamble
  CCA Method..... Energy Detect + Carrier
Detect/Correlation
  Data Retries..... 6
  Fragment Threshold..... 2342
  Radio Channels..... 36 40 44 48 52 56 60 64 149 153 157
161 165
  Tx Power Mode..... Automatic
  Rate List (MB)..... 6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0

```

Related Commands

[config client ccx get-client-capability](#)
[config client ccx get-manufacturer-info](#)
[config client ccx get-operating-parameters](#)
[config client ccx get-profiles](#)

show client ccx results

To view the results from the last successful diagnostic test, use the **show client ccx results** command.

show client ccx results *client_mac_address*

Syntax Description	show	Display settings.
	client	Client settings.
	ccx	Cisco Compatible Extensions (CCX) settings.
	results	Display the results of the last successful diagnostic test for the CCX client.
	<i>client_mac_address</i>	Specifies the MAC address of the client.

Examples

Information similar to the following appears for the 802.1x authentication test:

```
dot1x Complete..... Success
EAP Method..... *1,Host OS Login Credentials
dot1x Status..... 255
```

Related Commands

[config client ccx test-abort](#)
[config client ccx test-association](#)
[config client ccx test-dot1x](#)
[config client ccx test-profile](#)
[config client ccx clear-reports](#)
[config client ccx clear-results](#)

show client ccx rm

To display CCX client radio management report information, use the **show client ccx rm** commands.

```
show client ccx rm client_MAC [ status |  
                                report ( chan-load | noise-hist | frame request | beacon | frame ) ]
```

Syntax Description

show	Display settings.
client	Client settings.
ccx	Cisco Compatible Extensions (CCX) settings.
rm	Radio management settings.
<i>client_MAC</i>	Specifies the client MAC address.
status	Displays client ccx radio management status information.
report	Displays client ccx radio management report.
chan-load	Displays radio management channel load reports.
noise-hist	Displays radio management noise histogram reports.
beacon	Displays radio management beacon load reports.
frame	Displays radio management frame reports.

Examples

```
> show client ccx rm 00:40:96:15:21:ac status
```

```
Client Mac Address..... 00:40:96:15:21:ac
Channel Load Request..... Enabled
Noise Histogram Request..... Enabled
Beacon Request..... Enabled
Frame Request..... Enabled
Interval..... 30
Iteration..... 10
```

```
> show client ccx rm 00:40:96:15:21:ac report chan-load
```

```
Channel Load Report
Client Mac Address..... 00:40:96:ae:53:bc
Timestamp..... 788751121
Incapable Flag..... On
Refused Flag..... On
Chan CCA Busy Fraction
-----
1    194
2    86
3    103
4     0
5    178
6    82
7    103
8    95
9    13
10   222
11   75
```

```

> show client ccx rm 00:40:96:15:21:ac report noise-hist
Noise Histogram Report
Client Mac Address..... 00:40:96:15:21:ac
Timestamp..... 4294967295
Incapable Flag..... Off
Refused Flag..... Off
Chan RPI0 RPI1 RPI2 RPI3 RPI4 RPI5 RPI6 RPI7

> show client ccx rm 00:40:96:ae:53:bc report beacon
Beacon Report
Client Mac Address..... 00:40:96:ae:53:bc
Timestamp..... 788853242
Incapable Flag..... On
Refused Flag..... On

Channel No..... 3
Phy Type..... ERP
Received signal Power..... -80dbm
BSSID..... 00:12:7f:50:93:10
Parent TFS..... bc729d5e
Parent TFS..... 42f637ec02000000
Beacon Interval..... 100
Capability Information..... 0401

Channel No..... 7
Phy Type..... ERP
Received signal Power..... -62dbm
BSSID..... 00:12:44:b3:b9:e0
Parent TFS..... 4f46aa5e
Parent TFS..... bd1ba60f00000000
Beacon Interval..... 100
Capability Information..... 0421

> show client ccx rm 00:40:96:ae:53:bc report frame
Frame Report
Client Mac Address..... 00:40:96:ae:53:bc
Timestamp..... 789140437
Incapable Flag..... On
Refused Flag..... On
Chan Tx Address Bssid RcxSigPwr Frame Count
-----

```

Related Commands

```

config client ccx default-gw-ping
config client ccx dhcp
config client ccx dns-ping
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
config client ccx send-message

```

show client ccx stats-report

To display the CCX statistics report from a specified client device, use the **show client ccx stats-report** command.

show client ccx stats-report *client_mac_address*

Syntax Description

show	Display settings.
client	Client settings.
ccx	Cisco Compatible Extensions (CCX) settings.
stats-report	Display a CCX client statistics report.
<i>client_mac_address</i>	Displays the MAC address for the specified client device.

Defaults

None.

Examples

```
> config client ccx stats-request 1 dot11 00:40:96:a8:f7:98
> show client ccx stats-report 00:40:96:a8:f7:98
```

```
Measurement duration = 1
```

```
dot11TransmittedFragmentCount      = 1
dot11MulticastTransmittedFrameCount = 2
dot11FailedCount                   = 3
dot11RetryCount                     = 4
dot11MultipleRetryCount             = 5
dot11FrameDuplicateCount            = 6
dot11RTSSuccessCount                = 7
dot11RTSFailureCount                = 8
dot11ACKFailureCount                = 9
dot11ReceivedFragmentCount          = 10
dot11MulticastReceivedFrameCount    = 11
dot11FCSErrorCount                  = 12
dot11TransmittedFrameCount          = 13
```

Related Commands

```
config client ccx default-gw-ping
config client ccx dhcp
config client ccx dns-ping
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
config client ccx send-message
```


show client detail

To display detailed information for a client on a Cisco lightweight access point, use the **show client detail** command.

show client detail *mac_address*

Syntax Description

show	Display settings.
client	Display client settings.
detail	Connectivity information.
<i>mac_address</i>	MAC address of the specific client.

Usage Guidelines

The [show client ap](#) command may list the status of automatically disabled clients. Use the [show exclusionlist](#) command to view clients on the exclusion list (blacklisted).

Examples

```
> show client detail 00:0c:41:07:33:a6

Client MAC Address..... 00:16:36:40:ac:58
Client Username..... N/A
Client State..... Associated
Client NAC OOB State..... QUARANTINE
Guest LAN Id..... 1
IP Address..... Unknown
Session Timeout..... 0
QoS Level..... Gold
Diff Serv Code Point (DSCP)..... disabled
Mobility State..... Local
Internal Mobility State..... apfMsMmInitial
Security Policy Completed..... No
Policy Manager State..... WEBAUTH_REQD
Policy Manager Rule Created..... Yes
NPU Fast Fast Notified..... Yes
Last Policy Manager State..... WEBAUTH_REQD
Client Entry Create Time..... 460 seconds
Interface..... wired-guest
VLAN..... 236
Quarantine VLAN..... 0
Client Statistics:
  Number of Bytes Received..... 0
  Number of Bytes Sent..... 0
  Number of Packets Received..... 0
  Number of Packets Sent..... 0
  Number of EAP Id Request Msg Timeouts..... 0
  Number of EAP Id Request Msg Failures..... 0
  Number of EAP Request Msg Timeouts..... 2
  Number of EAP Request Msg Failures..... 1
  Number of EAP Key Msg Timeouts..... 0
  Number of EAP Key Msg Failures..... 0
  Number of Policy Errors..... 0
  Radio Signal Strength Indicator..... Unavailable
  Signal to Noise Ratio..... Unavailable
...
```

Related Commands

[Show Client Commands](#)

[Configure Client Commands](#)

show client location-calibration summary

To display client location calibration summary information, use the **show client location-calibration summary** command.

show client location-calibration summary

Syntax Description

show	Display settings.
client	Display client settings.
location-calibration	Display client location calibration information.
summary	Summarize client location calibration information.

Examples

```
> show client location-calibration summary
```

```
MAC Address Interval
-----
10:10:10:10:10:10 60
21:21:21:21:21:21 45
```

Related Commands

[Show Client Commands](#)
[Configure Client Commands](#)

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_addr*

Syntax Description

show	Display settings.
client	Display client settings.
roam-history	Display roaming history information for a specified client.
<i>mac_addr</i>	MAC address of specified client.

Examples

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

Related Commands

[Show Client Commands](#)
[Configure Client Commands](#)

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

show	Display settings.
client	802.11a or 802.11b/g client.
summary	All attached clients.

Usage Guidelines

The [show client ap](#) command may list the status of automatically disabled clients. Use the [show exclusionlist](#) command to view clients on the exclusion list (blacklisted).

Examples

```
> show client summary
```

```
Number of Clients..... 24
```

MAC Address	AP Name	Status	WLAN	Auth	Protocol	Port
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11a	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11a	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11b	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11a	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11b	1
xx:xx:xx:xx:xx:xx	AP02	Associated	2	Yes	802.11b	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11b	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11b	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11b	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11a	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11a	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11b	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11a	1
xx:xx:xx:xx:xx:xx	AP02	Probing	N/A	No	802.11a	1

```
Number of Clients..... 2
```

Related Commands

[Show Client Commands](#)
[Configure Client Commands](#)

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

show	Display settings.
client	802.11a or 802.11b/g client.
summary	All attached clients.
guest-LAN	Indicates the active wired guest LAN.

Examples

```
> show client summary
```

```
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 Commands](#)
[Configure Client Commands](#)

show client username

To display client data by username, use the **show client username** command.

show client username *username*

Syntax Description

show	Display settings.
client	Displays client data.
username	Cisco radio.
<i>username</i>	Client's username.

Examples

```
> 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 country

To display the configured country and the radio types supported, use the **show country channels** command.

show country

This command has no arguments or keywords.

Examples

```
> show country
```

```
Configured Country..... United States
Configured Country Codes
  US - United States..... 802.11a / 802.11b / 802.11g
```

Related Commands

config country
display country supported
show country channels

show country supported

To display a list of the supported country options, use the **show country supported** command.

show country supported

Syntax Description This command has no arguments or keywords.

Examples

```
> show country supported
CConfigured Country..... United States
Supported Country Codes
AR - Argentina..... 802.11a / 802.11b / 802.11g
AT - Austria..... 802.11a / 802.11b / 802.11g
AU - Australia..... 802.11a / 802.11b / 802.11g
BR - Brazil..... 802.11a / 802.11b / 802.11g
BE - Belgium..... 802.11a / 802.11b / 802.11g
BG - Bulgaria..... 802.11a / 802.11b / 802.11g
CA - Canada..... 802.11a / 802.11b / 802.11g
CH - Switzerland..... 802.11a / 802.11b / 802.11g
CL - Chile..... 802.11b / 802.11g
CN - China..... 802.11a / 802.11b / 802.11g
CO - Colombia..... 802.11b / 802.11g
CY - Cyprus..... 802.11a / 802.11b / 802.11g
CZ - Czech Republic..... 802.11a / 802.11b
DE - Germany..... 802.11a / 802.11b / 802.11g
DK - Denmark..... 802.11a / 802.11b / 802.11g
EE - Estonia..... 802.11a / 802.11b / 802.11g
ES - Spain..... 802.11a / 802.11b / 802.11g
FI - Finland..... 802.11a / 802.11b / 802.11g
FR - France..... 802.11a / 802.11b / 802.11g
GB - United Kingdom..... 802.11a / 802.11b / 802.11g
GI - Gibraltar..... 802.11a / 802.11b / 802.11g
GR - Greece..... 802.11a / 802.11b / 802.11g
HK - Hong Kong..... 802.11a / 802.11b / 802.11g
HU - Hungary..... 802.11a / 802.11b / 802.11g
ID - Indonesia..... 802.11b / 802.11g
IE - Ireland..... 802.11a / 802.11b / 802.11g
IN - India..... 802.11a / 802.11b / 802.11g
IL - Israel..... 802.11a / 802.11b / 802.11g
ILO - Israel (outdoor)..... 802.11b / 802.11g
IS - Iceland..... 802.11a / 802.11b / 802.11g
IT - Italy..... 802.11a / 802.11b / 802.11g
JP - Japan (J)..... 802.11a / 802.11b / 802.11g
J2 - Japan 2(P)..... 802.11a / 802.11b / 802.11g
J3 - Japan 3(U)..... 802.11a / 802.11b / 802.11g
KR - Korea Republic (C)..... 802.11a / 802.11b / 802.11g
KE - Korea Extended (K)..... 802.11a / 802.11b / 802.11g
LI - Liechtenstein..... 802.11a / 802.11b / 802.11g
LT - Lithuania..... 802.11a / 802.11b / 802.11g
LU - Luxembourg..... 802.11a / 802.11b / 802.11g
LV - Latvia..... 802.11a / 802.11b / 802.11g
MC - Monaco..... 802.11a / 802.11b / 802.11g
MT - Malta..... 802.11a / 802.11b / 802.11g
MX - Mexico..... 802.11a / 802.11b / 802.11g
MY - Malaysia..... 802.11a / 802.11b / 802.11g
NL - Netherlands..... 802.11a / 802.11b / 802.11g
NZ - New Zealand..... 802.11a / 802.11b / 802.11g
NO - Norway..... 802.11a / 802.11b / 802.11g
```

PA	- Panama.....	802.11b / 802.11g
PE	- Peru.....	802.11b / 802.11g
PH	- Philippines.....	802.11a / 802.11b / 802.11g
PL	- Poland.....	802.11a / 802.11b / 802.11g
PT	- Portugal.....	802.11a / 802.11b / 802.11g
RU	- Russian Federation.....	802.11a / 802.11b / 802.11g
RO	- Romania.....	802.11a / 802.11b / 802.11g
SA	- Saudi Arabia.....	802.11a / 802.11b / 802.11g
SE	- Sweden.....	802.11a / 802.11b / 802.11g
SG	- Singapore.....	802.11a / 802.11b / 802.11g
SI	- Slovenia.....	802.11a / 802.11b / 802.11g
SK	- Slovak Republic.....	802.11a / 802.11b / 802.11g
TH	- Thailand.....	802.11b / 802.11g
TR	- Turkey.....	802.11b / 802.11g
TW	- Taiwan.....	802.11a / 802.11b / 802.11g
UA	- Ukraine.....	802.11a / 802.11b / 802.11g
US	- United States.....	802.11a / 802.11b / 802.11g
USL	- United States (Legacy).....	802.11a / 802.11b / 802.11g
USX	- United States (US + chan165).....	802.11a / 802.11b / 802.11g
VE	- Venezuela.....	802.11b / 802.11g
ZA	- South Africa.....	802.11a / 802.11b / 802.11g

Related Commands

config country
display country channels
show country

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.

Examples

```
> 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	<pre>> show cpu Current CPU load: 2.50%</pre>

Related Commands	show sysinfo

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.

Examples

> **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**

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.

Examples

```
> 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 debug

Use the **show debug** command to determine if MAC address and other flag debugging is enabled or disabled.

show debug

Syntax Description

show	Display settings.
debug	MAC address debugging.

Examples

```
> show debug

MAC debugging..... disabled

Debug Flags Enabled:
  arp error enabled.
  bcast error enabled.
```

Related Commands

debug mac

show dhcp

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

show dhcp { **leases** | **summary** | *scope* }

Syntax Description

show	Display settings.
dhcp	Dynamic Host Configuration Protocol settings.
leases	Enter leases to display allocated DHCP leases.
summary	Enter summary to display DHCP summary information.
<i>scope</i>	Enter the name of a scope to display the DHCP information for that scope.

Examples

```
> show dhcp leases
```

```
No leases allocated.
```

```
> show dhcp summary
```

```
Scope Name          Enabled          Address Range
003                  No              0.0.0.0 -> 0.0.0.0
```

```
> 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](#)
[config dhcp proxy](#)
[config interface dhcp](#)
[config wlan dhcp_server](#)
[debug dhcp](#)
[debug dhcp service-port](#)
[debug disable-all](#)
[show dhcp proxy](#)

show dtls connections

Use the **show dtls connections** command to display the Datagram Transport Layer Security (DTLS) server status.

show dtls connections

Syntax Description

show	Display settings.
dtls connections	DTLS server status.

Examples

> **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

Related Commands

[config ap link-encryption](#)

show dhcp proxy

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

show dhcp proxy

Syntax Description

show	Display settings.
dhcp	Dynamic Host Configuration Protocol settings.
proxy	Displays the status of DHCP proxy handling.

Examples

```
> show dhcp proxy
```

```
DHCP Proxy Behaviour: enabled
```

Related Commands

[config dhcp](#)
[config dhcp proxy](#)
[config interface dhcp](#)
[config wlan dhcp_server](#)
[debug dhcp](#)
[debug dhcp service-port](#)
[debug disable-all](#)
[show dhcp](#)

show eventlog

To display the event log, use the **show eventlog** command.

show eventlog

Syntax Description

show	Display settings.
eventlog	System events.

Examples

```
> show eventlog
```

	File	Line	TaskID	Code	Time			
					d	h	m	s
EVENT>	bootos.c	788	125CEBCC	AAAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125CEBCC	AAAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAAA	0	0	0	6
EVENT>	bootos.c	788	125C597C	AAAAAAAA	0	0	0	6
EVENT>	bootos.c	788	1216C36C	AAAAAAAA	0	0	0	6
EVENT>	bootos.c	788	1216C36C	AAAAAAAA	0	0	0	6
EVENT>	bootos.c	788	1216C36C	AAAAAAAA	0	0	0	6
EVENT>	bootos.c	788	1216C36C	AAAAAAAA	0	0	0	11

Related Commands

show msglog

show exclusionlist

To display a summary of all clients on the manual exclusion list (blacklisted) from associating with this Cisco Wireless LAN controller, use the **show exclusionlist** command.

show exclusionlist

Syntax Description

show	Display settings.
exclusionlist	Manual exclusion list.

Usage Guidelines

This command displays all manually excluded MAC addresses.

Examples

```
> show exclusionlist
```

MAC Address	Description
-----	-----
xx:xx:xx:xx:xx:xx	Disallowed Client

Related Commands

config exclusionlist add
config exclusionlist delete
config exclusionlist description
show client

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	show	Display settings.
	guest-lan	Indicates the active wired guest LAN.
	guest_lan_id	ID of selected wired guest LAN.

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

```
Examples
> 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 **show guest-lan summary**
show client summary guest-lan

show hreap group detail

To display the details for a specific hybrid-REAP group, use the **show hreap group detail** command.

show hreap group detail *group_name*

Syntax	Description
show	Display settings.
hreap	Hybrid Remote Edge Access Point settings.
group	Hybrid-REAP group settings.
detail	Hybrid-REAP group configuration details.
<i>group_name</i>	IP address of hybrid-REAP group.

Examples

```
> show hreap group detail 192.12.1.2
```

```
Number of Ap's in Group: 1
00:0a:b8:3b:0b:c2  AP1200  Joined
```

```
Group Radius Auth Servers:
  Primary Server Index ..... Disabled
  Secondary Server Index ..... Disabled
```

Related Commands

[config hreap group](#)
[show hreap group summary](#)

show hreap group summary

To display the current list of hybrid-REAP groups, use the **show hreap group summary** command.

show hreap group summary

Syntax Description

show	Display settings.
hreap	Hybrid Remote Edge Access Point settings.
group	Hybrid-REAP group settings.
summary	Displays a summary of the hybrid-REAP group.

Examples

```
> show hreap group summary
```

```
HREAP Group Summary: Count 1
```

Group Name	# APs
Group 1	1

Related Commands

[config hreap group](#)
[show hreap group detail](#)

show hreap office-extend

To display hybrid-REAP OfficeExtend access point information, use the **show hreap office-extend** command.

show hreap office-extend {summary | latency}

Syntax Description

show	Display settings.
hreap	Hybrid Remote Edge Access Point settings.
office-extend	OfficeExtend settings.
summary	Displays a list of all OfficeExtend access points.
latency	Displays the link delay for OfficeExtend access points .

Examples

```
> show hreap office-extend summary
Summary of OfficeExtend AP
AP Name           Ethernet MAC           Encryption  Join-Mode  Join-Time
-----
AP1130            00:22:90:e3:37:70     Enabled    Latency    Sun Jan 4 21:46:07 2009
AP1140            01:40:91:b5:31:70     Enabled    Latency    Sat Jan 3 19:30:25 2009

> show hreap office-extend latency
Summary of OfficeExtend AP link latency
AP Name           Status  Current  Maximum  Minimum
-----
AP1130            Enabled 15 ms    45 ms    12 ms
AP1140            Enabled 14 ms    179 ms   12 ms
```

Related Commands

[config hreap group](#)
[show hreap group detail](#)

show ike

To display active Internet Key Exchange (IKE) security associations (SAs), use the **show ike** command.

```
show ike { brief | detailed } IP_or_MAC_address
```

Syntax Description	show	Display settings.
	ike	Display Internet Key Exchange security associations.
	brief	Brief summary of all active IKE SAs.
	detailed	Detailed summary of all active IKE SAs.
	<i>IP_or_MAC_address</i>	IP or MAC address of active IKE SA.

Examples	> show ike brief 10.10.10.10

Related Commands	None.

show interface

Use the **show interface** command to display details of the system interfaces.

show interface {**summary** | **detailed** *interface_name*}

Syntax Description

show interface	Command action
summary	Displays a summary of the local interfaces.
detailed	Displays detailed interface information.
<i>interface_name</i>	Identifies interface name for detailed display

Examples

> **show interface summary**

Interface Name	Port	Vlan Id	IP Address	Type	Ap	Mgr	Guest
ap-manager	1	untagged	xxx.xxx.xxx.xxx	Static	Yes	No	
management	1	untagged	xxx.xxx.xxx.xxx	Static	No	No	
service-port	N/A	N/A	xxx.xxx.xxx.xxx	Static	No	No	
virtual	N/A	N/A	xxx.xxx.xxx.xxx	Static	No	No	



Note The interface name of the wired guest LAN in the following example is management and its VLAN ID is 149.

> **show interface detailed management**

```
Interface Name..... management
MAC Address..... 00:0b:85:32:ab:60
IP Address..... 1.100.49.30
IP Netmask..... 255.255.255.0
IP Gateway..... 1.100.49.1
VLAN..... 149
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port..... Unconfigured
Primary DHCP Server..... 1.100.2.15
Secondary DHCP Server..... Unconfigured
ACL..... Unconfigured
AP Manager..... No
```



Note

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

Related Commands

[Configure Interface Commands](#)

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

show	Display settings.
invalid-config	Display any CLI commands in the configuration file with invalid values.

Usage Guidelines



Note You can execute this command only before the [clear config](#) or [save config](#) command.

Examples

To see a list of any ignored commands or invalid configuration values in a configuration file, enter this command:

```
> show invalid-config
```

```
config wlan peer-blocking drop 3
config wlan dhcp_server 3 192.168.0.44 required
```

Related Commands

None.

show inventory

To display a physical inventory of the Cisco Wireless LAN controller, use the **show inventory** command.

show inventory

Syntax Description

show	Display settings.
inventory	Physical Cisco Wireless LAN controller configuration.

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

```
> 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 ipsec

To display active Internet Protocol Security (IPSec) security associations (SAs), use the **show ipsec** commands.

show ipsec {brief | detailed} *IP_or_MAC_address*

Syntax Description

show	Display settings.
ipsec	Internet Protocol Security security associations.
brief	Brief sumamry of active IPSec SAs.
detailed	Detailed summary of active IPSec SAs.
<i>IP_or_MAC_address</i>	Enter the IP address or MAC address of a device to see its IPSec SAs.

Examples

> **show ipsec brief 10.10.10.10**

Related Commands

[config radius acct ipsec authentication](#)
[config radius acct ipsec disable](#)
[config radius acct ipsec enable](#)
[config radius acct ipsec encryption](#)
[config radius acct ipsec ike](#)
[config radius auth ipsec authentication](#)
[config radius auth ipsec disable](#)
[config radius auth ipsec encryption](#)
[config radius auth ipsec ike](#)
[config trapflags ipsec](#)
[config wlan security ipsec disable](#)
[config wlan security ipsec enable](#)
[config wlan security ipsec authentication](#)
[config wlan security ipsec encryption](#)
[config wlan security ipsec config](#)
[config wlan security ipsec ike authentication](#)
[config wlan security ipsec ike dh-group](#)
[config wlan security ipsec ike lifetime](#)
[config wlan security ipsec ike phase1](#)
[config wlan security ipsec ike contivity](#)

show known ap

To display known Cisco lightweight access point information, use the **show known ap** command.

show known ap {**summary** | **detailed** *MAC*}

Syntax Description	show	Display settings.
	known ap	Known Cisco lightweight access point information.
	summary	Displays a list of all known access points.
	detailed	Provides detailed information for all known access points.
	<i>MAC</i>	MAC address of the known AP

Examples

```
> show known ap summary
```

MAC Address	State	# Aps	# Clients	Last Heard
-----	-----	-----	-----	-----

Related Commands

[config ap](#)

show l2tp

To display Layer 2 Tunneling Protocol (L2TP) sessions, use the **show l2tp** command.

```
show l2tp {summary | ip_address}
```

Syntax Description	show l2tp	Display settings.
	summary	Displays all L2TP sessions.
	ip_address	Displays an L2TP session.

Examples

```
> show l2tp summary

LAC_IPaddr  LTid  LSid  RTid  RSid  ATid  ASid  State
-----

```

Related Commands

None.

show lag summary

To display the current LAG status, use the **show lag summary** command.

show lag summary

Syntax Description	This command has no arguments or keywords.

Examples	<pre>> show lag summary</pre> LAG Enabled

Related Commands	config lag

show ldap

To display the Lightweight Directory Access Protocol (LDAP) server information for a particular LDAP server, use the **show ldap** command.

show ldap *index*

Syntax Description

show	Display settings.
ldap	Lightweight Directory Access Protocol server settings.
<i>index</i>	LDAP server index. Valid values are from 1 to 17.

Defaults

None.

Examples

```
> show ldap 1
Server Index..... 1
Address..... 2.3.1.4
Port..... 389
Enabled..... Yes
User DN..... name1
User Attribute..... attr1
User Type..... username1
Retransmit Timeout..... 3 seconds
Bind Method ..... Anonymous
```

Related Commands

[config ldap](#)
[config ldap add](#)
[config ldap simple-bind](#)
[show ldap statistics](#)
[show ldap summary](#)

show ldap statistics

To display all Lightweight Directory Access Protocol (LDAP) server information, use the **show ldap statistics** command.

show ldap statistics

Syntax Description	show	Display settings.
	ldap	Lightweight Directory Access Protocol server settings.
	statistics	Display detailed LDAP server settings.

Examples

```
> show ldap statistics

Server Index..... 1
Server statistics:
  Initialized OK..... 0
  Initialization failed..... 0
  Initialization retries..... 0
  Closed OK..... 0
Request statistics:
  Received..... 0
  Sent..... 0
  OK..... 0
  Success..... 0
  Authentication failed..... 0
  Server not found..... 0
  No received attributes..... 0
  No passed username..... 0
  Not connected to server..... 0
  Internal error..... 0
  Retries..... 0

Server Index..... 2
...
```

Related Commands

- [config ldap](#)
- [config ldap add](#)
- [config ldap simple-bind](#)
- [show ldap](#)
- [show ldap summary](#)

show ldap summary

To display the current Lightweight Directory Access Protocol (LDAP) server status, use the **show ldap summary** command.

show ldap summary

Syntax Description

show	Display settings.
ldap	Lightweight Directory Access Protocol server settings.
summary	Display detailed LDAP server settings.

Examples

```
> show ldap summary
```

Idx	Server Address	Port	Enabled
1	2.3.1.4	389	Yes
2	10.10.20.22	389	Yes

Related Commands

[config ldap](#)
[config ldap add](#)
[config ldap simple-bind](#)
[show ldap](#)
[show ldap statistics](#)

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	show	Display settings.
	license	License settings.
	agent { counters sessions }	Display license agent counter and session information.

Defaults None.

Examples

>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
```

>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

show	Display settings.
license	License settings.
all	Display all the licenses.

Defaults

None.

Examples

```
>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](#)
- [license modify priority](#)
- [show license agent](#)
- [show license detail](#)
- [show license feature](#)
- [show license image-level](#)
- [show license summary](#)

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

show	Display settings.
license	License settings.
capacity	Display license currently used by the access point.

Defaults

None.

Examples

```
>show license capacity
```

Licensed Feature	Max Count	Current Count	Remaining Count
AP Count	250	47	203

Related Commands

[license install](#)
[license modify priority](#)
[show license agent](#)
[show license all](#)
[show license detail](#)
[show license feature](#)
[show license image-level](#)
[show license summary](#)

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

show	Display settings.
license	License settings.
detail <i>license_name</i>	Display details of a specific license.

Defaults

None.

Examples

```
>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](#)
[license modify priority](#)
[show license agent](#)
[show license all](#)
[show license feature](#)
[show license image-level](#)
[show license summary](#)

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

show	Display settings.
license	License settings.
expiring	Display expiring licenses.

Defaults

None.

Examples

```
>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](#)
[license modify priority](#)
[show license all](#)
[show license detail](#)
[show license evaluation](#)
[show license in-use](#)
[show license summary](#)

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

show	Display settings.
license	License settings.
evaluation	Display evaluation licenses.

Defaults

None.

Examples

```
>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](#)
[license modify priority](#)
[show license all](#)
[show license detail](#)
[show license expiring](#)
[show license in-use](#)
[show license summary](#)

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

show	Display settings.
license	License settings.
feature	Display license enabled features.

Defaults

None.

Examples

```
>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](#)
[license modify priority](#)
[show license all](#)
[show license detail](#)
[show license expiring](#)
[show license evaluation](#)
[show license image-level](#)
[show license in-use](#)
[show license summary](#)

show license file

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

show license file

Syntax	Description
show	Display settings.
license	License settings.
file	Display all the license files.

Defaults None.

Examples

```
>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
m63lR5l8JM3DPkr4O2DI43iLlKn7jomo3RF1lLjMRqLkKHiLJ2tOyuftQsq2bCAO6
nR3wIb38xKi3t$<WLC>AQEBIQAB//++mCzRUbOhw28vz0czAY0iAm7ocDLUMB9ER0
+BD3w2PhNEYwsBN/T3xXBqJqfC+oKRgwInXo3s+nsLU7rOtdOxoIxYZAo3LYmUJ+M
Fzsq1hKoJVlPyEvQ8H2lMNUjVbhoN0gyIWsyiJaM8AQIkVBQFzhr10GYolVzdzfJf
EPQIx6tZ++/Vtc/q3SF/5Ko8XCXY=</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 handle

To display the license handles on the Cisco 5500 series controller, use the **show license handle** command.

show license handle

Syntax Description

show	Display settings.
license	License settings.
handle	Display license handles.

Defaults

None.

Examples

>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	show	Display settings.
	license	License settings.
	image-level	Display the image level.

Defaults None.

Examples

```
>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](#)
[license modify priority](#)
[show license all](#)
[show license detail](#)
[show license expiring](#)
[show license feature](#)
[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

show	Display settings.
license	License settings.
in-use	Display license that are in-use.

Defaults

None.

Examples

```
>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](#)
[license modify priority](#)
[show license all](#)
[show license detail](#)
[show license evaluation](#)
[show license expiring](#)
[show license feature](#)
[show license image-level](#)
[show license permanent](#)
[show license summary](#)

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	show	Display settings.
	license	License settings.
	permanent	Display permanent licenses.

Defaults	None.

Examples

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

show license status

To display license status on the Cisco 5500 series controller, use the **show license status** command.

show license status

Syntax Description

show	Display settings.
license	License settings.
status	Display license status.

Defaults

None.

Examples

```
>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](#)
[license modify priority](#)
[show license all](#)
[show license detail](#)
[show license evaluation](#)
[show license expiring](#)
[show license feature](#)
[show license image-level](#)
[show license permanent](#)
[show license summary](#)

show license statistics

To display license statistics on the Cisco 5500 series controller, use the **show license statistics** command.

show license statistics

Syntax Description

show	Display settings.
license	License settings.
statistics	Display license statistics.

Defaults

None.

Examples

```
>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
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](#)
[license modify priority](#)
[show license all](#)
[show license detail](#)
[show license evaluation](#)
[show license expiring](#)
[show license feature](#)
[show license image-level](#)
[show license permanent](#)
[show license summary](#)

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

show	Display settings.
license	License settings.
summary	Display brief summary of all licenses.

Defaults

None.

Examples

```
>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](#)
[license modify priority](#)
[show license all](#)
[show license detail](#)
[show license evaluation](#)
[show license expiring](#)
[show license feature](#)
[show license image-level](#)
[show license permanent](#)
[show license summary](#)

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	show	Display settings.
	license	License settings.
	udi	Display UDI values for licenses.

Defaults None.

Examples

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

Related Commands

[license install](#)
[license modify priority](#)
[show license all](#)
[show license detail](#)
[show license evaluation](#)
[show license expiring](#)
[show license feature](#)
[show license image-level](#)
[show license permanent](#)
[show license summary](#)

show load-balancing

To display the status of the load-balancing feature, use the **show load-balancing** command.

show load-balancing

Syntax Description	show	Display settings.
	load-balancing	Displays the load-balancing status.

Defaults	None.

Examples	<pre>> 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</pre>

Related Commands	config load-balancing

show local-auth certificates

This command is used to display local authentication certificate information:

show local-auth certificates

Syntax Description	show	Display settings.
	local-auth	Authentication certificate information stored locally.
	certificates	Display certificate information.

Examples

```
> show local-auth certificates
```

Certificates available for Local EAP authentication:

```
Certificate issuer ..... vendor
  CA certificate:
    Subject: C=AU, ST=NSW, L=Sydney, O=Cisco Systems
    OU=WNBU Sydney, CN=wnbu-syd-acs-a.cisco.com
    Issuer: C=AU, ST=NSW, L=Sydney, O=Cisco Systems
    OU=WNBU Sydney, CN=wnbu-syd-acs-a.cisco.com
    Valid: 2005 Jun 15th, 04:53:49 GMT to 2008 Jun 15th, 05:03:34 GMT
  Device certificate:
    Subject: MAILTO=test@test.net, C=AU, ST=NSW, L=Sydney
    O=Cisco Systems, OU=WNBU Sydney, CN=concanon
    Issuer: C=AU, ST=NSW, L=Sydney, O=Cisco Systems
    OU=WNBU Sydney, CN=wnbu-syd-acs-a.cisco.com
    Valid: 2006 Aug 9th, 05:14:16 GMT to 2007 Aug 9th, 05:24:16 GMT

Certificate issuer ..... cisco
  CA certificate:
    Subject: C=US, ST=California, L=San Jose, O=airespace Inc
    OU=none, CN=ca, MAILTO=support@airespace.com
    Issuer: C=US, ST=California, L=San Jose, O=airespace Inc
    OU=none, CN=ca, MAILTO=support@airespace.com
    Valid: 2003 Feb 12th, 23:38:55 GMT to 2012 Nov 11th, 23:38:55 GMT
  Device certificate:
    Subject: C=US, ST=California, L=San Jose, O=airespace Inc
    CN=000b85335340, MAILTO=support@airespace.com
    Issuer: C=US, ST=California, L=San Jose, O=airespace Inc
    OU=none, CN=ca, MAILTO=support@airespace.com
    Valid: 2005 Feb 22nd, 10:52:58 GMT to 2014 Nov 22nd, 10:52:58 GMT

Certificate issuer ..... legacy
  CA certificate:
    Subject: C=US, ST=California, L=San Jose, O=airespace Inc
    OU=none, CN=ca, MAILTO=support@airespace.com
    Issuer: C=US, ST=California, L=San Jose, O=airespace Inc
    OU=none, CN=ca, MAILTO=support@airespace.com
    Valid: 2003 Feb 12th, 23:38:55 GMT to 2012 Nov 11th, 23:38:55 GMT

  Device certificate:
    Subject: C=US, ST=California, L=San Jose, O=airespace Inc
    CN=000b85335340, MAILTO=support@airespace.com
    Issuer: C=US, ST=California, L=San Jose, O=airespace Inc
    OU=none, CN=ca, MAILTO=support@airespace.com
    Valid: 2005 Feb 22nd, 10:52:58 GMT to 2014 Nov 22nd, 10:52:58 GMT
```

Related Commands

clear stats local-auth
config local-auth active-timeout
config local-auth eap-profile
config local-auth method fast
config local-auth user-credentials
debug aaa local-auth
show local-auth config
show local-auth statistics

show local-auth config

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

show local-auth config

Syntax Description	show	Display settings.
	local-auth	Authentication certificate information stored locally.
	config	Display local authentication configuration information.

Examples

> **show local-auth config**

User credentials database search order:

Primary Local DB

Configured EAP profiles:

Name fast-test
 Certificate issuer default
 Enabled methods fast
 Configured on WLANs 2

EAP Method configuration:

EAP-TLS:

Certificate issuer default
 Peer verification options:
 Check against CA certificates Enabled
 Verify certificate CN identity Disabled
 Check certificate date validity ... Enabled

EAP-FAST:

TTL for the PAC 3 600
 Initial client message <none>
 Local certificate required No
 Client certificate required No
 Vendor certificate required No
 Anonymous provision allowed Yes
 Authenticator ID 7b7fffff000000000000000000000000
 Authority Information Test

EAP Profile..... tls-prof

Enabled methods for this profile tls
 Active on WLANs 1 3

EAP Method configuration:

EAP-TLS:

Certificate issuer used cisco
 Peer verification options:
 Check against CA certificates disabled
 Verify certificate CN identity disabled
 Check certificate date validity ... disabled

Related Commands

[clear stats local-auth](#)
[config local-auth active-timeout](#)
[config local-auth eap-profile](#)
[config local-auth method fast](#)

config local-auth user-credentials
debug aaa local-auth
show local-auth certificates
show local-auth statistics

show local-auth statistics

This command is used to display local EAP authentication statistics:

show local-auth statistics

Syntax Description	show	Display settings.
	local-auth	Authentication certificate information stored locally.
	statistics	Display local authentication certificate statistics.

Defaults None.

Examples

> **show local-auth statistics**

```
Local EAP authentication DB statistics:
Requests received ..... 14
Responses returned ..... 14
Requests dropped (no EAP AVP) ..... 0
Requests dropped (other reasons) ..... 0
Authentication timeouts ..... 0
```

```
Authentication statistics:
  Method          Success      Fail
  -----
  Unknown          0           0
  LEAP              0           0
  EAP-FAST         2           0
  EAP-TLS           0           0
  PEAP              0           0
```

```
Local EAP credential request statistics:
Requests sent to LDAP DB ..... 0
Requests sent to File DB ..... 2
Requests failed (unable to send) ..... 0
Authentication results received:
  Success ..... 2
  Fail ..... 0
Certificate operations:
Local device certificate load failures ..... 0
Total peer certificates checked ..... 0
Failures:
  CA issuer check ..... 0
  CN name not equal to identity ..... 0
  Dates not valid or expired ..... 0
```

Related Commands

[clear stats local-auth](#)
[config local-auth active-timeout](#)
[config local-auth eap-profile](#)
[config local-auth method fast](#)
[config local-auth user-credentials](#)

```
debug aaa local-auth  
show local-auth certificates  
show local-auth config
```

show location

To display location system information, use the **show location** command.

show location [**detail** *mac_address* | **summary**]

Syntax Description

show	Display settings.
location	Display location system settings.
detail	Displays detailed location information
<i>mac_address</i>	Specifies the MAC address of a client.
summary	Displays summary location information.

Examples

```
> show location summary
Location Summary

Algorithm used:                Average
Client
    RSSI expiry timeout:      5 sec
    Half life:                 0 sec
    Notify Threshold:         0 db
Calibrating Client
    RSSI expiry timeout:      5 sec
    Half life:                 0 sec
Rogue AP
    RSSI expiry timeout:      5 sec
    Half life:                 0 sec
    Notify Threshold:         0 db
RFID Tag
    RSSI expiry timeout:      5 sec
    Half life:                 0 sec
    Notify Threshold:         0 db
```

Related Commands

[clear location rfid](#)
[clear location statistics rfid](#)
[config location](#)
[show location statistics rfid](#)

show location statistics rfid

To see any radio frequency identification (RFID)-related errors, use the **show location statistics rfid** command.

show location statistics rfid

Syntax Description

show	Display settings.
location	Display location settings.
statistics	Displays detailed location information.
rfid	Display detailed location RFID statistics.

Examples

```
> show location statistics rfid
```

RFID Statistics

Database Full :	0	Failed Delete:	0
Null Bufhandle:	0	Bad Packet:	0
Bad LWAPP Data:	0	Bad LWAPP Encap:	0
Off Channel:	0	Bad CCX Version:	0
Bad AP Info :	0		
Above Max RSSI:	0	Below Max RSSI:	0
Invalid RSSI:	0	Add RSSI Failed:	0
Oldest Expired RSSI:	0	Smallest Overwrite:	0

Related Commands

[clear location rfid](#)
[clear location statistics rfid](#)
[config location](#)
[show location](#)

show logging

To display the syslog facility logging parameters and buffer contents, use the **show logging** command.

show logging

Syntax Description	show	Display settings.
	logging	Current settings and buffer content details.

Examples

> **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
--More-- or (q)uit
  - 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 loginsession

To display the existing sessions, use the **show loginsession** command.

show loginsession

Syntax Description

show	Display settings.
loginsession	Current session details.

Examples

```
> show loginsession
```

ID	User Name	Connection From	Idle Time	Session Time
00	admin	EIA-232	00:00:00	00:19:04

Related Commands

[config loginsession close](#)

show macfilter

To display the MAC filter parameters, use the **show macfilter** command. The MAC delimiter (none, colon, or hyphen) for MAC addresses sent to RADIUS servers is displayed. The MAC filter table lists the clients that are always allowed to associate with a wireless LAN.

show macfilter {**summary** | **detail** *MAC*}

Syntax Description

show	Display settings.
macfilter	Filter details.
summary	Displays a summary of all MAC filter entries.
detail <i>MAC</i>	Detailed display of a MAC filter entry.

Examples

```
> show macfilter detail xx:xx:xx:xx:xx:xx
```

```
MAC Address..... xx:xx:xx:xx:xx:xx
WLAN Identifier..... Any
Interface Name..... management
Description..... RAP
```

```
> show macfilter summary
```

```
MAC Filter RADIUS Compatibility mode..... Cisco ACS
MAC Filter Delimiter..... None
```

Local Mac Filter Table

MAC Address	WLAN Id	Description
xx:xx:xx:xx:xx:xx	Any	RAP
xx:xx:xx:xx:xx:xx	Any	PAP2 (2nd hop)
xx:xx:xx:xx:xx:xx	Any	PAP1 (1st hop)

Related Commands

[config macfilter](#)
[config macfilter description](#)
[config macfilter interface](#)
[config macfilter ip-address](#)
[config macfilter mac-delimiter](#)
[config macfilter radius-compatible](#)
[config macfilter wlan-id](#)

show memory monitor

To view a summary of memory analysis settings and any discovered memory issues, enter this command:

show memory monitor [detail]

Syntax Description	show	Display settings.
	memory	Controller memory leak settings.
	monitor	Display memory monitoring settings and monitor results summary.
	detail	(Optional) Display details of any memory leaks or corruption.



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, and you are collecting troubleshooting information.

Examples

To view a summary of memory monitoring settings and a summary of test results, enter this command:

> show memory monitor

Information similar to the following appears:

```
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.
```

To view the details of the monitor test results, enter this command:

> show memory monitor detail

Information similar to the following appears:

```
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 Mesh Commands

Use the SHOW MESH commands to display settings for outdoor and indoor mesh access points.

show mesh ap

To display settings for mesh access points, use the **show mesh** commands.

show mesh ap {summary | tree}

Syntax Description	show	Display settings.
	mesh	Mesh access point settings (indoor and outdoor).
	summary	Displays a summary of mesh access point information including name, model, bridge virtual interface (BVI) MAC address, United States Computer Emergency Response Team (US-CERT) MAC address, hop, and bridge group name.
	tree	Displays a summary of mesh access point information in a tree configuration, including name, hop counter, link signal-to-noise ratio (SNR), and bridge group name.

Examples

To display settings in a summary format, enter this command:

```
> show mesh ap summary
```

AP Name	AP Model	BVI MAC	CERT MAC	Hop	Bridge Group Name
SB_RAP1	AIR-LAP1522AG-A-K9	00:1d:71:0e:d0:00	00:1d:71:0e:d0:00	0	sbox
SB_MAP1	AIR-LAP1522AG-A-K9	00:1d:71:0e:85:00	00:1d:71:0e:85:00	1	sbox
SB_MAP2	AIR-LAP1522AG-A-K9	00:1b:d4:a7:8b:00	00:1b:d4:a7:8b:00	2	sbox
SB_MAP3	AIR-LAP1522AG-A-K9	00:1d:71:0d:ee:00	00:1d:71:0d:ee:00	3	sbox

Number of Mesh APs..... 4
 Number of RAPs..... 1
 Number of MAPs..... 3

To display settings in a hierarchical (tree) format, enter this command:

```
> show mesh ap tree
```

```
=====
||  AP Name [Hop Counter, Link SNR, Bridge Group Name]  ||
=====

[Sector 1]
-----
SB_RAP1[0,0,sbox]
  |-SB_MAP1[1,32,sbox]
    |-SB_MAP2[2,27,sbox]
      |-SB_MAP3[3,30,sbox]

-----
Number of Mesh APs..... 4
Number of RAPs..... 1
Number of MAPs..... 3
-----
```

Related Commands

[Configure Mesh Commands](#)

show mesh astools stats

To display anti-stranding statistics for outdoor mesh access points, use the **show mesh astools** command.

show mesh astools stats [*cisco_ap*]

Syntax Description

show	Display settings.
mesh	Mesh access point settings (indoor and outdoor).
astools	Global anti-stranding feature for outdoor mesh access points.
stats	Display global anti-stranding feature statistics.
<i>cisco_ap</i>	Optional. Display anti-stranding feature statistics for a designated mesh access point.

Defaults

None.

Examples

To view anti-stranding statistics on all outdoor mesh access points, enter this command:

```
> show mesh astools stats
```

```
Total No of Aps stranded : 0
```

To view anti-stranding statistics for access point *sb_map1*, enter this command:

```
> show mesh astools stats sb_map1
```

```
Total No of Aps stranded : 0
```

Related Commands

[config mesh astools](#)
[show mesh config](#)
[show mesh stats](#)

show mesh background-scanning

To show whether or not the background-scanning feature is enabled on a mesh network, use the **show mesh background-scanning** command.

show mesh background-scanning

Syntax Description

show	Display settings.
mesh	Mesh access point settings (indoor and outdoor).
background-scanning	Display state of background-scanning feature.

Usage Guidelines



Note The secondary backhaul access feature is not supported by Cisco 1520 and 1524 indoor mesh access points in the 5.2 release.

Examples

To view the state of the background-scanning feature, enter this command:

```
> show mesh background-scanning
```

```
Background Scanning State: enabled
```

Related Commands

[config mesh background-scanning](#)
[show mesh config](#)
[show mesh stats](#)

show mesh backhaul rate-adapt

To show whether or not clients on a mesh network have access to the backhaul channel, and at what level of service, use the **show mesh backhaul rate-adapt** command.

show mesh backhaul rate-adapt

Syntax Description	show	Display settings.
	mesh	Mesh access point settings (indoor and outdoor).
	backhaul	Display state of backhaul feature.
	rate-adapt	Display at what service level the backhaul client access is set: • All allows clients <i>universal access</i> privileges. • Bronze allows <i>background-level</i> client access privileges. • Silver allows <i>best effort-level</i> client access privileges. • Gold allows <i>video-level</i> client access privileges. • Platinum allows <i>voice-level</i> client access privileges.

Examples To view the state of the backhaul rate-adaption feature, enter this command:

```
> show mesh backhaul rate-adapt

Bronze Queue..... Disabled
Gold Queue..... Enabled
Platinum Queue..... Disabled
Silver Queue..... Disabled
```

Related Commands [config mesh backhaul rate-adapt](#)
[show mesh config](#)
[show mesh stats](#)

show mesh cac

To display call admission control (CAC) topology and the bandwidth used or available in a mesh network, use the **show mesh cac** commands.

show mesh cac {**summary** | {**bwused** {**voice** | **video**} | **access** | **callpath** | **rejected**} *cisco_ap*}

Syntax Description	
show	Display settings.
mesh	Mesh access point settings (indoor and outdoor).
cac	Call admission control settings.
summary	Total number of voice calls and voice bandwidth used for each mesh access point.
bwused	Display bandwidth for a selected access point in a tree topology.
access	Display access voice calls in progress in a tree topology.
callpath	Display the call bandwidth distributed across the mesh tree.
rejected	Display voice calls rejected for insufficient bandwidth in a tree topology.
voice	Displays the mesh topology and the voice bandwidth used or available.
video	Displays the mesh topology and the video bandwidth used or available.
<i>cisco_ap</i>	Specifies the mesh access point name.

Examples

> **show mesh cac summary**

AP Name	Slot#	Radio	BW Used/Max	Calls
SB_RAP1	0	11b/g	0/23437	0
	1	11a	0/23437	0
SB_MAP1	0	11b/g	0/23437	0
	1	11a	0/23437	0
SB_MAP2	0	11b/g	0/23437	0
	1	11a	0/23437	0
SB_MAP3	0	11b/g	0/23437	0
	1	11a	0/23437	0

> **show mesh cac bwused voice SB_MAP1**

AP Name	Slot#	Radio	BW Used/Max
SB_RAP1	0	11b/g	0/23437
	1	11a	0/23437
SB_MAP1	0	11b/g	0/23437
	1	11a	0/23437
SB_MAP2	0	11b/g	0/23437
	1	11a	0/23437
SB_MAP3	0	11b/g	0/23437
	1	11a	0/23437

```
> show mesh cac access 1524_Map1
```

AP Name	Slot#	Radio	Calls
-----	-----	-----	-----
1524_Rap	0	11b/g	0
	1	11a	0
	2	11a	0
1524_Map1	0	11b/g	0
	1	11a	0
	2	11a	0
1524_Map2	0	11b/g	0
	1	11a	0
	2	11a	0

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 video tspec-inactivity-timeout
config 802.11 cac voice acm
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 cac voice load-based
config 802.11 cac voice stream-size
debug cac

```

show mesh client-access

To display the backhaul client access configuration setting, use the **show mesh client-access** command.

show mesh client-access

Syntax Description

show	Display settings.
mesh	Mesh access point settings (indoor and outdoor).
client-access	Display backhaul client access configuration settings.

Examples

```
> show mesh client-access
Backhaul with client access status: enabled
```

Related Commands

[config mesh client-access](#)

show mesh config

To display mesh configuration settings, use the **show mesh config** command.

show mesh config

Syntax Description

show	Display settings.
mesh	Mesh access point settings (indoor and outdoor).
config	Display global mesh configuration settings.

Examples

To display global mesh configuration settings, enter this command:

```
(Sandbox_WLC_01) >show mesh config
```

```
Mesh Range..... 12000
Backhaul with client access status..... disabled
Background Scanning State..... enabled

Mesh Security
  Security Mode..... EAP
  External-Auth..... disabled
  Use MAC Filter in External AAA server..... disabled
  Force External Authentication..... disabled

Mesh Alarm Criteria
  Max Hop Count..... 4
  Recommended Max Children for MAP..... 10
  Recommended Max Children for RAP..... 20
  Low Link SNR..... 12
  High Link SNR..... 60
  Max Association Number..... 10
  Association Interval..... 60 minutes
  Parent Change Numbers..... 3
  Parent Change Interval..... 60 minutes

Mesh Multicast Mode..... In-Out
Mesh Full Sector DFS..... enabled

Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

Related Commands

[Configure Mesh Commands](#)

show mesh env

To display global or specific environment summary information for mesh networks, use the **show mesh env** command.

show mesh env {**summary** | *cisco_ap*}

Syntax Description

show	Display settings.
mesh	Mesh access point settings (indoor and outdoor).
env	Display mesh environment settings.
summary	Display global environment summary information.
<i>cisco_ap</i>	Name of access point for which environment summary information is requested.

Examples

> **show mesh env summary**

AP Name	Temperature(C)	Heater	Ethernet	Battery
ap1130:5f:be:90	N/A	N/A	DOWN	N/A
AP1242:b2.31.ea	N/A	N/A	DOWN	N/A
AP1131:f2.8d.92	N/A	N/A	DOWN	N/A
AP1131:46f2.98ac	N/A	N/A	DOWN	N/A
ap1500:62:39:70	-36	OFF	UP	N/A

> **show mesh env SB_RAP1**

```

AP Name..... SB_RAP1
AP Model..... AIR-LAP1522AG-A-K9
AP Role..... RootAP

Temperature..... 21 C, 69 F
Heater..... OFF
Backhaul..... GigabitEthernet0

GigabitEthernet0 Status..... UP
  Duplex..... FULL
  Speed..... 100
  Rx Unicast Packets..... 114754
  Rx Non-Unicast Packets..... 1464
  Tx Unicast Packets..... 9630
  Tx Non-Unicast Packets..... 3331
GigabitEthernet1 Status..... DOWN
  POE Out..... OFF

Battery..... N/A

```

Related Commands

[Configure Mesh Commands](#)

show mesh neigh

To display summary or detailed information about the mesh neighbors for a specific mesh access point, use the **show mesh neigh** command.

```
show mesh neigh {detail | summary} {cisco_ap | all}
```

Syntax Description

show	Display configurations.
mesh	Mesh configuration.
neigh	Display mesh access point neighbors.
detail summary	- Enter detail to view the channel and signal-to-noise ratio (SNR) details between the designated mesh access point and its neighbor. - Enter summary to view the mesh neighbors for a designated mesh access point.
cisco_ap	Cisco lightweight access point name.
all	All access points.

Examples

To view a neighbor summary of access point *ap1500:62:39:70*, enter this command:

```
> show mesh neighbor summary ap1500:62:39:70
```

AP Name/Radio	Mac	Channel	Snr-Up	Snr-Down	Link-Snr	Flags	State
mesh-45-rap1	165	15	18	16	0x86b	UPDATED NEIGH	PARENT BEACON
00:0B:85:80:ED:D0	149	5	6	5	0x1a60	NEED UPDATE	BEACON DEFAULT
00:17:94:FE:C3:5F	149	7	0	0	0x860	BEACON	

To view detailed neighbor statistics of access point *ap1500:62:39:70*, enter this command:

```
> show mesh neigh detail ap1500:62:39:70
```

Related Commands

- [show mesh config](#)
- [show mesh env](#)

show mesh path

To display the channel and signal-to-noise ratio (SNR) details for a link between a mesh access point and its neighbor, use the **show mesh path** command.

show mesh path *cisco_ap*

Syntax Description

show	Display configurations.
mesh	Mesh configuration.
path	Show channel and SNR details for a designated link path.
<i>cisco_ap</i>	Mesh access point name.

Examples

> **show mesh path mesh-45-rap1**

```

AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
mesh-45-rap1      165      15      18      16      0x86b UPDATED NEIGH PARENT BEACON
mesh-45-rap1 is a Root AP.
```

Related Commands

[config mesh backhaul rate-adapt](#)
[config mesh client-access](#)
[config mesh linktest](#)
[config mesh range](#)
[show mesh config](#)
[show mesh neigh](#)
[show mesh stats](#)

show mesh per-stats

To display the percentage of packet errors for packets transmitted by the neighbors of a specified mesh access point, use the **show mesh per-stats** command.

show mesh per-stats summary { *cisco_ap* | **all** }

Syntax Description

show	Display settings.
mesh	Mesh access point settings (indoor and outdoor).
per-stats	Percentage of packet errors transmitted via neighbor access points.
summary	Packet Error Rate stats summary.
<i>cisco_ap</i>	Name of mesh access point.
all	All mesh access points.

Usage Guidelines

The packet error rate percentage equals 1, which is the number of successfully transmitted packets divided by the number of total packets transmitted.

Examples

To display the percentage of packet errors for packets transmitted by the neighbors to mesh access point *ap_12*, enter this command:

```
> show mesh per-stats summary ap_12
```

```
Neighbor MAC Address 00:0B:85:5F:FA:F0
Total Packets transmitted: 104833
Total Packets transmitted successfully: 104833
Total Packets retried for transmission: 33028
Neighbor MAC Address: 00:0B:85:80:ED:D0
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
Neighbor MAC Address: 00:17:94:FE:C3:5F
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
```

Related Commands

[config mesh linktest](#)
[config mesh range](#)
[show mesh config](#)
[show mesh neigh](#)
[show mesh stats](#)

show mesh queue-stats

To view the number of packets in a client access queue by type for a particular mesh access point, use the **show mesh queue-stats** command.

show mesh queue-stats { *cisco_ap* | **all** }

Syntax Description

show	Display settings.
mesh	Mesh access point settings (indoor and outdoor).
queue-stats	Packet queue statistics for client access queues.
<i>cisco_ap</i>	Name of access point for which you want packet queue statistics.
all	All access points.

Examples

To show packet queue statistics for access point ap417, enter this command:

```
> show mesh queue-stats ap417
```

```
Queue Type Overflows Peak length Average length
-----
Silver      0           1           0.000
Gold        0           4           0.004
Platinum    0           4           0.001
Bronze      0           0           0.000
Management 0           0           0.000
```

Related Commands

[config mesh client-access](#)
[config mesh multicast](#)
[config mesh secondary-backhaul](#)
[show mesh client-access](#)
[show mesh config](#)
[show mesh stats](#)
[show mgmtuser](#)

show mesh public-safety

To display 4.8-GHz public safety settings, use the **show mesh public-safety** command.

show mesh public-safety

Syntax Description	show	Display settings.
	mesh	Mesh access point settings (indoor and outdoor).
	public-safety	Display 4.8-GHz public safety channel settings.

Examples

To view 4.8-GHz public safety settings, enter this command:

> **show mesh public-safety**

Global Public Safety status: disabled

Related Commands

[config 802.11-a](#)
[config 802.11-a antenna extAntGain](#)
[config 802.11-a channel ap](#)
[config 802.11-a txpower ap](#)
[config mesh public-safety](#)
[config mesh security](#)
[show mesh ap](#)
[show mesh security-stats](#)
[show mesh stats](#)

show mesh secbh-stats

To display queue statistics for secondary backhaul access in a mesh network, use the **show mesh secbh-stats** command.

show mesh secbh-stats { *cisco_ap* | **all** }

Syntax Description

show	Display settings.
mesh	Mesh access point settings (indoor and outdoor).
secbh-stats	Secondary backhaul statistics.
<i>cisco_ap</i>	Mesh access point selected for display statistics.
all	All mesh access points.



Usage Guidelines

Note The secondary backhaul access feature is not supported by Cisco 1520 and 1524 indoor mesh access points in the 5.2 release.

Examples

To display statistics for secondary backhaul access of access point *SB_RAP1*, enter this command:

```
> show mesh secbh-stats SB_RAP1
```

```
Radio Type: 802.11BG
Queue:Silver:
  Packet retries: 0
  Packets dropped after max retries: 0
Queue:Gold:
  Packet retries: 0
  Packets dropped after max retries: 0
Queue:Platinum:
  Packet retries: 0
  Packets dropped after max retries: 0
```

```
Radio Type: 802.11A
Queue:Silver:
  Packet retries: 0
  Packets dropped after max retries: 0
Queue:Gold:
  Packet retries: 0
  Packets dropped after max retries: 0
Queue:Platinum:
  Packet retries: 0
  Packets dropped after max retries: 0
```

Related Commands

[config mesh secondary-backhaul](#)
[show mesh secondary-backhaul](#)

show mesh secondary-backhaul

To display the current state of mesh secondary backhaul configuration settings, use the **show mesh secondary-backhaul** command.

show mesh secondary-backhaul

Syntax Description

show	Display settings.
mesh	Mesh access point settings (indoor and outdoor).
secondary-backhaul	Secondary backhaul configuration settings.

Usage Guidelines



Note The secondary backhaul access feature is not supported by Cisco 1520 and 1524 indoor mesh access points in the 5.2 release.

Examples

```
> show mesh secondary-backhaul

MESH secondary-backhaul: enabled
```

Related Commands

[config mesh secondary-backhaul](#)
[show mesh secbh-stats](#)

show mesh security-stats

To display packet error statistics for a specific access point, use the **show mesh security-stats** command.

show mesh security-stats {*cisco_ap* | **all**}

Syntax Description

show	Display settings.
mesh	Mesh access point settings (indoor and outdoor).
<i>cisco_ap</i>	Name of access point for which you want packet error statistics.
all	All access points.

Usage Guidelines

This command shows packet error statistics and a count of failures, timeouts, and successes with respect to associations and authentications as well as reassociations and reauthentications for the specified access point and its child.

Examples

To show packet error statistics for access point ap417, enter this command:

```
> show mesh security-stats ap417

AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
-----
x Packets 14, Rx Packets 19, Rx Error Packets 0
Parent-Side Statistics:
-----
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Child-Side Statistics:
-----
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
Re-Association Timeouts 0
Re-Association Successes 0
Re-Authentication Failures 0
Re-Authentication Timeouts 0
Re-Authentication Successes 0
```

Related Commands

[config mesh alarm](#)
[config mesh linkdata](#)
[config mesh linktest](#)
[config mesh security](#)

show mesh stats

To display the mesh statistics for a Cisco lightweight access point, use the **show mesh stats** command.

show mesh stats *cisco_ap*

Syntax Description	show	Display configurations.
	mesh	Mesh configuration.
	stats	Show Cisco lightweight access point statistics.
	<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults None.

Examples

> **show mesh stats RAP_ap1**

```
RAP in state Maint
rxNeighReq 759978, rxNeighRsp 568673
txNeighReq 115433, txNeighRsp 759978
rxNeighUpd 8266447 txNeighUpd 693062
tnextchan 0, nextant 0, downAnt 0, downChan 0, curAnts 0
tnextNeigh 0, malformedNeighPackets 244, poorNeighSnr 27901
blacklistPackets 0, insufficientMemory 0
authenticationFailures 0
Parent Changes 1, Neighbor Timeouts 16625
```

Related Commands

[config mesh alarm](#)
[config mesh client-access](#)
[config mesh ethernet-bridging vlan-transparent](#)
[config mesh linkdata](#)
[config mesh linktest](#)
[config mesh security](#)
[show mesh per-stats](#)
[show mesh queue-stats](#)
[show mesh security-stats](#)

show mgmtuser

To display the local management user accounts on the Cisco Wireless LAN controller, use the **show mgmtuser** command.

show mgmtuser

Syntax Description

show	Display settings.
mgmtuser	List of management users.

Examples

> **show mgmtuser**

User Name	Permissions	Description
-----	-----	-----
admin	read-write	

Related Commands

config mgmtuser add
config mgmtuser delete
config mgmtuser password

Show Mobility Commands

Use the **show mobility** commands to display mobility settings.

show mobility anchor

To display the wireless LAN anchor export list for the Cisco Wireless LAN controller mobility groups or to display a list and status of controllers configured as mobility anchors for a specific WLAN or wired guest LAN, use the **show mobility anchor** commands.

show mobility anchor [**wan** *wlan_id* | **guest-lan** *guest_lan_id*]

Syntax Description

show	Display settings.
mobility	Mobility group.
anchor	Displays the mobility wireless LAN anchor list.
wlan	Wireless LAN mobility group settings.
<i>wlan_id</i>	A wireless LAN identifier between 1 and 512 (inclusive).
guest-lan	Guest LAN mobility group settings.
<i>guest_lan_id</i>	A guest LAN identifier between 1 and 5 (inclusive).

Defaults

None.

Usage Guidelines

The status field display (see example) shows one of the following values:

- **UP**—The controller is reachable and able to pass data.
- **CNTRL_PATH_DOWN**—The mpings failed. The controller cannot be reached through the control path and is considered failed.
- **DATA_PATH_DOWN**—The epings failed. The controller cannot be reached and is considered failed.
- **CNTRL_DATA_PATH_DOWN**—Both the mpings and epings failed. The controller cannot be reached and is considered failed.

Examples

```
> show mobility anchor
```

Mobility Anchor Export List

WLAN ID	IP Address	Status
-----	-----	-----
12	192.168.0.15	UP

GLAN ID	IP Address	Status
-----	-----	-----
1	192.168.0.9	CNTRL_DATA_PATH_DOWN

Related Commands

[config guest-lan mobility 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 mobility statistics reset
- config wlan mobility anchor
- debug mobility
- show mobility anchor
- show mobility statistics
- show mobility summary

show mobility statistics

To display the statistics information for the Cisco Wireless LAN controller mobility groups, use the **show mobility statistics** command.

show mobility statistics

Syntax Description	show	Display settings.
	mobility	Mobility group.
	statistics	Displays statistics for the mobility manager.

Defaults	None.

Examples

```
> show mobility statistics

Global Mobility Statistics
  Rx Errors..... 0
  Tx Errors..... 0
  Responses Retransmitted..... 0
  Handoff Requests Received..... 0
  Handoff End Requests Received..... 0
  State Transitions Disallowed..... 0
  Resource Unavailable..... 0
Mobility Initiator Statistics
  Handoff Requests Sent..... 0
  Handoff Replies Received..... 0
  Handoff as Local Received..... 2
  Handoff as Foreign Received..... 0
  Handoff Denys Received..... 0
  Anchor Request Sent..... 0
  Anchor Deny Received..... 0
  Anchor Grant Received..... 0
  Anchor Transfer Received..... 0
Mobility Responder Statistics
  Handoff Requests Ignored..... 0
  Ping Pong Handoff Requests Dropped..... 0
  Handoff Requests Dropped..... 0
  Handoff Requests Denied..... 0
  Client Handoff as Local..... 0
  Client Handoff as Foreign ..... 0
  Client Handoff Inter Group ..... 0
  Anchor Requests Received..... 0
  Anchor Requests Denied..... 0
  Anchor Requests Granted..... 0
  Anchor Transferred..... 0
```

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 mobility statistics reset
debug mobility
show mobility anchor
show mobility summary

show mobility summary

To display the summary information for the Cisco Wireless LAN controller mobility groups, use the **show mobility summary** command.

show mobility summary

Syntax Description

show	Display settings.
mobility	Mobility group.
summary	Displays a summary of the mobility manager.

Defaults

None.

Examples

> **show mobility summary**

```
Symmetric Mobility Tunneling (current) ..... Disabled
Symmetric Mobility Tunneling (after reboot) ..... Disabled
Mobility Protocol Port..... 16666
Mobility Security Mode..... Disabled
Default Mobility Domain..... snmp_gui
Multicast Mode ..... Disabled
Mobility Domain ID for 802.11r..... 0x66bd
Mobility Keepalive Interval..... 10
Mobility Keepalive Count..... 3
Mobility Group Members Configured..... 1
Mobility Control Message DSCP Value..... 0

Controllers configured in the Mobility Group
MAC Address      IP Address      Group Name      Multicast IP Status
00:1b:d4:6b:87:20  1.100.163.70   snmp_gui        0.0.0.0         Up
```



Note

Some WLAN controllers may list no mobility security mode.

Related Commands

[config guest-lan mobility 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 mobility statistics reset](#)
[config wlan mobility anchor](#)
[debug mobility](#)
[show mobility anchor](#)
[show mobility statistics](#)

show msglog

To display the message logs written to the Cisco Wireless LAN controller database, use the **show msglog** command. If there are more than 15 entries you are prompted to display the messages shown in the example.

show msglog

Syntax Description	show	Display settings.
	msglog	Shows message logs.

Defaults	None.

Examples

```
> show msglog
```

```
Message Log Severity Level..... ERROR
Thu Aug  4 14:30:08 2005 [ERROR] spam_lrad.c 1540: AP 00:0b:85:18:b6:50 associated. Last
AP failure was due to Link Failure
Thu Aug  4 14:30:08 2005 [ERROR] spam_lrad.c 13840: Updating IP info for AP 00:
0b:85:18:b6:50 -- static 0, 1.100.49.240/255.255.255.0, gtw 1.100.49.1
Thu Aug  4 14:29:32 2005 [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Thu Aug  4 14:29:32 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11a switch group
reset
Thu Aug  4 14:29:32 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Thu Aug  4 14:29:22 2005 [ERROR] sim.c 2841: Unable to get link state for primary port 0
of interface ap-manager
Thu Aug  4 14:29:22 2005 [ERROR] dtl_l2_dot1q.c 767: Unable to get USP
Thu Aug  4 14:29:22 2005 Previous message occurred 2 times
Thu Aug  4 14:29:14 2005 [CRITICAL] osapi_sem.c 794: Error! osapiMutexTake called with
NULL pointer: osapi_bsntime.c:927
Thu Aug  4 14:29:14 2005 [CRITICAL] osapi_sem.c 794: Error! osapiMutexTake called with
NULL pointer: osapi_bsntime.c:919
Thu Aug  4 14:29:14 2005 [CRITICAL] hwutils.c 1861: Security Module not found
Thu Aug  4 14:29:13 2005 [CRITICAL] bootos.c 791: Starting code...
```

Related Commands	show eventlog

show nac statistics

To display detailed Network Access Control (NAC) information about a Cisco Wireless LAN controller, use the **show nac statistics** command.

show nac statistics

Syntax Description	show	Display settings.
	nac	Network access control.
	statistics	Detailed statistics.

Defaults	None.

Examples

```
> show nac statistics

Server Index..... 1
Server Address..... xxx.xxx.xxx.xxx
Number of requests sent..... 0
Number of retransmissions..... 0
Number of requests received..... 0
Number of malformed requests received..... 0
Number of bad auth requests received..... 0
Number of pending requests..... 0
Number of timed out requests..... 0
Number of misc dropped request received..... 0
Number of requests sent..... 0
```

Related Commands

- [show nac summary](#)
- [config guest-lan nac](#)
- [config wlan nac](#)
- [debug nac](#)

show nac summary

To display NAC summary information for a Cisco Wireless LAN controller, use the **show nac summary** command.

show nac summary

Syntax Description

show	Display settings.
nac	Network Access Control.
summary	Summary information.

Examples

```
> show nac summary

NAC ACL Name .....
Index  Server Address                Port      State
-----
1      xxx.xxx.xxx.xxx                13336     Enabled
```

Related Commands

- [show nac statistics](#)
- [config guest-lan nac](#)
- [config wlan nac](#)
- [debug nac](#)

show netuser

This command is used display detailed login information about a specified netuser or displays a summary information on all network users.

To show the configuration of a particular user in the local user database—**show netuser detail** *username*.

To list all users in the local user database—**show netuser summary**.

Syntax Description

detail	Displays detailed information on the specified network user.
<i>username</i>	Specifies a network username (up to 24 alphanumeric characters).
summary	Displays summary information on all network users.

Examples

```
> show netuser summary
```

```
Maximum logins allowed for a given user name .....Unlimited
```

```
> show netuser detail john10
```

```
User Name..... abc
WLAN Id..... Any
Lifetime..... Permanent
Description..... test user
```

Related Commands

[Configure Net User Commands](#)
[show netuser guest-roles](#)

show netuser guest-roles

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

show netuser guest-roles

Syntax Description

show	Displays parameters.
netuser	Local network user.
guest-role	QoS role for the guest user.

Examples

```
> 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

[Configure Net User Commands](#)
[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	show	Display settings.
	network	802.3 bridging settings.

Defaults	None.

Examples	<pre>> show network</pre>

Related Commands	Configure Network Commands 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

show	Display settings.
network	Network configuration settings.
summary	Summary of network configuration.

Defaults

None.

Examples

```
> 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 Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable   Mode: Ucast
Ethernet Broadcast Mode..... Disable
IGMP snooping..... Disabled
IGMP timeout..... 60 seconds
User Idle Timeout..... 300 seconds
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
```

Related Commands

[Configure Network Commands](#)
[show network](#)
[show network multicast mgid detail](#)
[show network multicast mgid summary](#)

show network multicast mgid detail

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

show network multicast mgid detail *mgid_value*

Syntax Description

show	Display settings.
network	Network configuration.
<i>mgid_value</i>	Number between 550 and 4095.

Defaults

None.

Examples

```
> 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

[Configure Network Commands](#)
[show network](#)
[show network summary](#)
[show network multicast mgid summary](#)

show network multicast mgid summary

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

show network multicast mgid summary

Syntax Description

show	Display settings.
network	Network configuration.

Examples

```
> 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

- [Configure Network Commands](#)
- [show network](#)
- [show network summary](#)
- [show network multicast mgid detail](#)

show nmsp notify-interval summary

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

Syntax Description	This command has no arguments or keywords.

Examples	<pre>>show nmsp notify-interval summary</pre>

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

show nmosp statistics

To display Network Mobility Services Protocol (NMSP) counters, use the **show nmosp statistics** command.

show nmosp statistics {summary | connection all}

Syntax Description

show	Display settings.
nmosp	Network Mobility Services Protocol settings.
statistics	Display NMSP counters.
summary	Display common NMSP counters.
connection all	Display all connection-specific counters.

Examples

To display a summary of common NMSP counters, enter this command:

```
> show nmosp 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
```

To display all the connection-specific NMSP counters, enter this command:

```
> show nmosp 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 Rsp:	0
Loc Subscr Req:	0	Loc Subscr Rsp:	0
Loc Notif:	0		
Loc Unsubscr Req:	0	Loc Unsubscr Rsp:	0
IDS Get Req:	0	IDS Get Resp:	0
IDS Notif:	0		
IDS Set Req:	0	IDS Set Resp:	0

Related Commands

[clear nmsp statistics](#)
[config nmsp notify-interval measurement](#)
[show nmsp notify-interval summary](#)
[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.

Examples

```
>show nmsp status
```

LocServer	IP	TxEchoResp	RxEchoReq	TxData	RxData
171.71.132.158	21642	21642	51278	21253	

Related Commands

[clear locp statistics](#)
[clear nmsp statistics](#)
[config nmsp notify-interval measurement](#)
[show nmsp notify-interval summary](#)
[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

show	Display settings.
nmosp	Network Mobility Services Protocol settings.
subscription	Display NMSP counters.
summary	Display all of the NMSP services to which the controller is subscribed.
detail	Display details for all of the NMSP services to which the controller is subscribed.
<i>ip_addr</i>	Display details only for the NMSP services subscribed to by a specific IP address.

Examples

```
>show nmsp subscription summary
```

```
Mobility Services Subscribed:
```

```
Server IP      Services
-----
10.10.10.31    RSSI, Info, Statistics
```

```
>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

[clear locp statistics](#)
[clear nmosp statistics](#)
[config nmosp notify-interval measurement](#)
[show nmosp notify-interval summary](#)
[show nmosp statistics](#)

show pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show port** command.

```
show pmk-cache {all | MAC}
```

Syntax Description	show	Display settings.
	pmk-cache	PMK cache settings.
	all	Displays information about all entries in the PMK cache.
	MAC	Displays information about a single entry in the PMK cache.

Examples

```
> show pmk-cache xx:xx:xx:xx:xx:xx

> show pmk-cache all

PMK Cache
Station          Entry
-----          -
Lifetime        VLAN Override    IP Override
-----          -
```

Related Commands [config pmk-cache delete](#)

show port

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

show port {*port* | **summary**}

Syntax Description

show	Display settings.
port	Cisco Wireless LAN controller port.
<i>port</i> summary	Individual port or all ports.

Examples

> **show port 1**

Pr	Type	STP Stat	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	Mcast Appliance	POE
1	Normal	Disa	Enable	Auto	1000 Full	Down	Enable	Enable	N/A



Note

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

> **show port summary**

Pr	Type	STP Stat	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	Mcast Appliance	POE
1	Normal	Forw	Enable	Auto	1000 Full	Up	Enable	Enable	N/A
2	Normal	Disa	Enable	Auto	1000 Full	Down	Enable	Enable	N/A
3	Normal	Disa	Enable	Auto	1000 Full	Down	Enable	Enable	N/A
4	Normal	Disa	Enable	Auto	1000 Full	Down	Enable	Enable	N/A



Note

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

Related Commands

[clear stats port](#)
[config ap port](#)
[config interface port](#)
[config network web-auth-port](#)
[Configure Port Commands](#)
[config spanningtree port mode](#)
[config spanningtree port pathcost](#)
[config spanningtree port priority](#)
[show stats port](#)

show process

To display how various processes in the system are using the CPU at that instant in time, use the **show process** commands.

show process {cpu | memory}

Syntax Description

show	Display settings.
process	System task settings.
cpu	Display how various system tasks are using the CPU at that moment.
memory	Display the allocation and deallocation of memory from various processes in the system at that moment.

Usage Guidelines

This command is helpful in understanding if any single task is monopolizing the CPU and preventing other tasks from being performed.

Examples

To show how various tasks in the system are using the CPU at a given moment, enter this command:

```
> 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

To show the allocation and deallocation of memory from various processes at a given moment, enter this command:

```
> 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 qos queue_length all

To display quality of service (QoS) information (queue length), use the **show qos** command.

show qos queue_length all

Syntax Description	show	Display settings.
	qos	Quality of Service information.
	queue_length all	Displays queue lengths.

Examples

```
> show qos queue_length all
```

```
Platinum queue length..... 255
Gold queue length..... 255
Silver queue length..... 150
Bronze queue length..... 100
```

Related Commands	config qos

Show Radius Commands

Use the **show radius** commands to display RADIUS settings.

show radius acct statistics

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

show radius acct statistics

Syntax Description	show	Display settings.
	radius acct	RADIUS accounting server.
	statistics	Displays RADIUS accounting server statistics.

Defaults None.

Examples

```
> show radius acct statistics

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

Related Commands

- [config advanced probe filter](#)
- [config advanced probe limit](#)
- [config radius acct fallback-test](#)
- [show advanced probe](#)
- [show radius auth statistics](#)
- [show radius summary](#)

show radius auth statistics

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

show radius auth statistics

Syntax Description	show	Display settings.
	radius auth	RADIUS authentication server.
	statistics	Displays RADIUS authentication server statistics.

Defaults	None.

Examples

```
> show radius auth statistics
```

Authentication Servers:

```

Server Index..... 1
Server Address..... 1.1.1.1
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0

```

Related Commands	show radius acct statistics
	show radius summary

show radius rfc3576 statistics

To display the RADIUS rfc3576 server statistics for the Cisco Wireless LAN controller, use the **show radius rfc3576 statistics** command.

show radius rfc3576 statistics

Syntax Description

show	Display settings.
radius rfc3576	RADIUS RFC3576 server.
statistics	Displays RADIUS RFC-3576 server statistics.

Usage Guidelines

RFC 3576, an extension to the RADIUS protocol, allows dynamic changes to a user session. This includes support for disconnecting users and changing authorizations applicable to a user session; that is, it provides support for Disconnect and Change-of-Authorization (CoA) messages. Disconnect messages cause a user session to be terminated immediately, whereas CoA messages modify session authorization attributes such as data filters.

Examples

```
> show radius rfc3576 statistics
```

```

RFC-3576 Servers:
Server Index..... 1
Server Address..... 10.1.17.10
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 0
Retry Requests..... 0
Accounting Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknown type Msgs..... 0
Other Drops..... 0

```

Related Commands

show radius auth statistics
show radius summary
show radius rfc3576

show radius summary

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

show radius summary

Syntax Description	show	Display settings.
	radius	RADIUS authentication server.
	summary	Server summary.

Defaults None.

Examples

```
> show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Credentials Caching..... Disabled
Call Station Id Type..... IP Address
Administrative Authentication via RADIUS..... Enabled
```

Authentication Servers

Index	Type	Server Address	Port	State	Tout	RFC-3576	IPSec - AuthMod
e/Phase1/Group/Lifetime/Auth/Encr							
----	----	-----	-----	-----	----	-----	-----

Accounting Servers

Index	Type	Server Address	Port	State	Tout	RFC-3576	IPSec - AuthMod
e/Phase1/Group/Lifetime/Auth/Encr							
----	----	-----	-----	-----	----	-----	-----

Related Commands

- show radius auth statistics**
- show radius acct statistics**

Show Radio Frequency ID Commands

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

show rfid client

To list the 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.

Usage Guidelines

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

Examples

When the RFID tag is in client mode, information similar to the following appears:

> **show rfid client**

RFID Mac	VENDOR	Heard Sec Ago	Associated AP	Chnl	Client State
00:14:7e:00:0b:b1	Pango	35	AP0019.e75c.fef4	1	Probing

Related Commands

config rfid
show rfid config
show rfid detail
show rfid summary

show rfid config

This command is used to display the current RFID configuration settings.

show rfid config

Syntax Description	This command has no arguments or keywords.

Examples

```
> 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 show rfid detail show rfid summary

show rfid detail

This command is used to display detailed RFID information for a specified tag.

show rfid detail *mac_address*

Syntax Description

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

Examples

```
> show rfid detail 32:21:3a:51:01:02

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
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
show rfid config

show rfid summary

This command is used to display detailed RFID information for a specified tag.

show rfid summary

Syntax Description This command has no arguments or keywords.

Examples

```
> 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
- show rfid config
- show rfid detail

Show Rogue Commands

Use the **show rogue** commands to display unverified (rogue) device settings.

show rogue adhoc detailed

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

show rogue adhoc detailed *MAC*

Syntax Description

show	Display settings.
rogue adhoc	Ad-hoc rogue.
detailed	Displays detailed information.
MAC	Ad-hoc rogue MAC address.

Examples

```
> show rogue adhoc detailed 02:61:ce:8e:a8:8c
```

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

Related Commands

[config rogue adhoc](#)
[config rogue rule](#)
[show rogue adhoc summary](#)
[show rogue ignore-list](#)
[show rogue rule detailed](#)
[show rogue rule summary](#)

show rogue adhoc summary

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

show rogue adhoc summary

Syntax Description

show	Display settings.
rogue adhoc	Ad-hoc rogue access point.
summary	Displays a list of all Adhoc Rogues.

Examples

```
> show rogue adhoc summary
Detect and report Ad-Hoc Networks..... Enabled

Client MAC Address   Adhoc BSSID   State  # APs   Last Heard
-----
xx:xx:xx:xx:xx:xx   super        Alert    1   Sat Aug  9 21:12:50 2004
xx:xx:xx:xx:xx:xx        Alert    1   Aug  9 21:12:50 2003
xx:xx:xx:xx:xx:xx        Alert    1   Sat Aug  9 21:10:50 2003
```

Related Commands

[config rogue adhoc](#)
[config rogue rule](#)
[show rogue adhoc detailed](#)
[show rogue ignore-list](#)
[show rogue rule detailed](#)
[show rogue rule summary](#)

show rogue ap clients

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

show rogue ap clients *ap_mac_address*

Syntax Description

show	Display settings.
rogue ap	Rogue access point.
clients	Summary information.
<i>ap_mac_address</i>	Rogue access point MAC address.

Examples

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

Related Commands

- [config rogue ap classify](#)
- [config rogue ap friendly](#)
- [config rogue ap rldp](#)
- [config rogue ap ssid](#)
- [config rogue ap timeout](#)
- [config rogue ap valid-client](#)
- [config rogue rule](#)
- [config trapflags rogueap](#)
- [show rogue ap detailed](#)
- [show rogue ap summary](#)
- [show rogue ap friendly summary](#)
- [show rogue ap malicious summary](#)
- [show rogue ap unclassified summary](#)

show rogue ap detailed

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

show rogue ap detailed *ap_mac_address*

Syntax Description

show	Display settings.
rogue ap	Rogue access point.
detailed	Displays detailed information.
<i>ap_mac_address</i>	Rogue access point MAC address.

Examples

```
> show rogue ap detailed xx:xx:xx:xx:xx:xx
```

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

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](#)
[config rogue rule](#)
[show rogue ap clients](#)
[show rogue ap summary](#)
[show rogue ap friendly summary](#)
[show rogue ap malicious summary](#)
[show rogue ap unclassified summary](#)

show rogue ap summary

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

show rogue ap summary

Syntax Description

show	Display settings.
rogue ap	Rogue access point.
summary	Displays a list of all rogue access points.

Examples

```
> show rogue ap summary
```

```
Rogue Location Discovery Protocol..... Disabled
Rogue ap timeout..... 1200
```

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

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](#)
[config rogue rule](#)
[show rogue ap clients](#)
[show rogue ap detailed](#)
[show rogue ap friendly summary](#)
[show rogue ap malicious summary](#)
[show rogue ap unclassified summary](#)

show rogue ap friendly summary

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

show rogue ap friendly summary

Syntax Description

show	Display settings.
rogue ap	Rogue access point.
friendly	Friendly rogue access points
summary	Displays a list of all rogue access points.

Examples

```
> show rogue ap friendly summary
```

```
Number of APs..... 1
MAC Address          State          # APs # Clients Last Heard
-----
XX:XX:XX:XX:XX:XX Internal          1      0 Tue Nov 27 13:52:04 2007
```

Related Commands

[config rogue ap classify](#)
[config rogue ap friendly](#)
[config rogue ap rldp](#)
[config rogue ap ssid](#)
[config rogue ap timeout](#)
[config rogue ap valid-client](#)
[config rogue rule](#)
[config trapflags rogueap](#)
[show rogue ap clients](#)
[show rogue ap detailed](#)
[show rogue ap summary](#)
[show rogue ap malicious summary](#)
[show rogue ap unclassified summary](#)

show rogue ap malicious summary

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

show rogue ap malicious summary

Syntax Description

show	Display settings.
rogue ap	Rogue access point.
malicious	Malicious rogue access points
summary	Displays a list of all rogue access points.

Examples

```
> show rogue ap malicious summary
```

```
Number of APs..... 2
MAC Address          State          # APs # Clients Last Heard
-----
XX:XX:XX:XX:XX:XX Alert              1      0 Tue Nov 27 13:52:04 2007
XX:XX:XX:XX:XX:XX Alert              1      0 Tue Nov 27 13:52:04 2007
```

Related Commands

[config rogue ap classify](#)
[config rogue ap friendly](#)
[config rogue ap rldp](#)
[config rogue ap ssid](#)
[config rogue ap timeout](#)
[config rogue ap valid-client](#)
[config rogue rule](#)
[config trapflags rogueap](#)
[show rogue ap clients](#)
[show rogue ap detailed](#)
[show rogue ap summary](#)
[show rogue ap friendly summary](#)
[show rogue ap unclassified summary](#)

show rogue ap unclassified summary

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

show rogue ap unclassified summary

Syntax Description

show	Display settings.
rogue ap	Rogue access point.
unclassified	Unclassified rogue access points
summary	Displays a list of all rogue access points.

Examples

```
> show rogue ap unclassified summary
```

```
Number of APs..... 164
MAC Address      State          # APs # Clients Last Heard
-----
XX:XX:XX:XX:XX:XX Alert          1      0    Fri Nov 30 11:12:52 2007
XX:XX:XX:XX:XX:XX Alert          1      0    Fri Nov 30 11:29:01 2007
XX:XX:XX:XX:XX:XX Alert          1      0    Fri Nov 30 11:26:23 2007
XX:XX:XX:XX:XX:XX Alert          1      0    Fri Nov 30 11:26:23 2007
```

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](#)
- [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 client detailed

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

show rogue client detailed *MAC*

Syntax Description	show	Display settings.
	rogue client	Rogue client.
	detailed	Provide detailed information for a rogue client.
	<i>MAC</i>	Rogue client MAC address.

Examples

```
> show rogue client detailed xx:xx:xx:xx:xx:xx

Rogue BSSID..... 00:0b:85:23:ea:d1
State..... Alert
First Time Rogue was Reported..... Mon Dec 3 21:50:36 2007
Last Time Rogue was Reported..... Mon Dec 3 21:50:36 2007
Rogue Client IP address..... Not known
Reported By
  AP 1
    MAC Address..... 00:15:c7:82:b6:b0
    Name..... AP0016.47b2.31ea
    Radio Type..... 802.11a
    RSSI..... -71 dBm
    SNR..... 23 dB
    Channel..... 149
    Last reported by this AP..... Mon Dec 3 21:50:36 2007
```

Related Commands

- [show rogue client summary](#)
- [show rogue ignore-list](#)
- [config rogue client](#)
- [config rogue rule](#)

show rogue client summary

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

show rogue client summary

Syntax Description

show	Display settings.
rogue client	Rogue client.
summary	Displays a list of all rogue clients.

Examples

> **show rogue client summary**

MAC Address	State	#	APs	Last	Heard
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:09:11	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:03:11	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:03:11	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:09:11	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	18:57:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:12:08	2005

Related Commands

[show rogue client detailed](#)
[show rogue ignore-list](#)
[config rogue client](#)
[config rogue rule](#)

show rogue ignore-list

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

show rogue ignore-list

Syntax Description

show	Display settings.
rogue ignore-list	Rogue access points that are configured to be ignored.
summary	Displays a list of all rogue clients.

Examples

```
> show rogue client summary
```

```
MAC Address
-----
XX:XX:XX:XX:XX:XX
```

Related Commands

[config rogue adhoc](#)
[config rogue ap classify](#)
[config rogue ap friendly](#)
[config rogue ap rldp](#)
[config rogue ap ssid](#)
[config rogue ap timeout](#)
[config rogue ap valid-client](#)
[config rogue client](#)
[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 client detailed](#)
[show rogue client summary](#)
[show rogue ignore-list](#)
[show rogue rule detailed](#)
[show rogue rule summary](#)

show rogue rule detailed

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

show rogue rule detailed *rule_name*

Syntax Description

show	Display settings.
rogue rule	Rogue rules.
detailed	Shows detailed information on a specific rogue classification rule.
<i>rule_name</i>	Rogue rule name.

Examples

> **show rogue rule detailed Rule2**

```

Priority..... 2
Rule Name..... Rule2
State..... Enabled
Type..... Malicious
Match Operation..... Any
Hit Count..... 352
Total Conditions..... 2
Condition 1
    type..... Client-count
    value..... 10
Condition 2
    type..... Duration
    value (seconds)..... 2000
Condition 3
    type..... Managed-ssid
    value..... Enabled
Condition 4
    type..... No-encryption
    value..... Enabled
Condition 5
    type..... Rssi
    value (dBm)..... -50
Condition 6
    type..... Ssid
    SSID Count..... 1
    SSID 1..... test

```

Related Commands

[config rogue rule](#)
[show rogue ignore-list](#)
[show rogue rule summary](#)

show rogue rule summary

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

show rogue rule summary

Syntax Description

show	Display settings.
rogue rule	Rogue rules.
summary	Displays a list of all rogue rules that are configured on the controller

Examples

> **show rogue rule summary**

Priority	Rule Name	State	Type	Match	Hit	Count
1	mtest	Enabled	Malicious	All	0	
2	asdfasdf	Enabled	Malicious	All	0	

Related Commands

[config rogue rule](#)
[show rogue ignore-list](#)
[show rogue rule detailed](#)

show route summary

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

show route summary

Syntax Description	show route	Command action.
	summary	Displays all the configured routes.

Examples

> 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 rules

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

show rules

Syntax Description	show rules	Displays active internal firewall rules.

Examples

```
> show rules

-----
Rule ID.....: 3
Ref count.....: 0
Precedence.....: 99999999
Flags.....: 00000001 ( PASS )
Source IP range:
    (Local stack)
Destination IP range:
    (Local stack)
-----
Rule ID.....: 25
Ref count.....: 0
Precedence.....: 99999999
Flags.....: 00000001 ( PASS )
Service Info
    Service name.....: GDB
    Protocol.....: 6
    Source port low.....: 0
    Source port high.....: 0
    Dest port low.....: 1000
    Dest port high.....: 1000
Source IP range:
IP High.....: 0.0.0.0
    Interface.....: ANY
Destination IP range:
    (Local stack)
-----
...

```

Related Commands	None.

show run-config

To show 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	show	Display settings.
	run-config	Show all controller configuration settings.
	no-ap	(Optional) Exclude access point configuration settings.
	commands	(Optional) Display a list of user-configured commands on the controller.



Usage Guidelines	Note	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 commands** command show only values configured by the user. It does not show system-configured default values.

Examples

```
> 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 serial

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

show serial

Syntax Description	show	Display settings.
	serial	Displays EIA-232 parameters and serial port inactivity timeout.

Defaults	9600, 8, off, 1, none.

Examples	<pre>> show serial Serial Port Login Timeout (minutes)..... 45 Baud Rate..... 9600 Character Size..... 8 Flow Control:..... Disable Stop Bits..... 1 Parity Type:..... none</pre>

Related Commands	config serial baudrate
	config serial timeout

show sessions

To show the console port login timeout and maximum number of simultaneous Command Line Interface (CLI) sessions, use the **show sessions** command.

show sessions

Syntax Description	show	Display settings.
	sessions	Displays CLI session configuration information.

Defaults 5 minutes, 5 sessions.

Examples

```
> 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 SNMP community entries, use the **show snmpcommunity** command.

show snmpcommunity

Syntax Description

show	Display settings.
snmpcommunity	Displays SNMP community entries.

Examples

```
> 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 version
config snmp community mode
config snmp community accessmode
config snmp community create
config snmp community delete
config snmp community ipaddr

```

show snmptrap

To show the Cisco Wireless LAN controller SNMP trap receivers and their status, use the **show snmptrap** command.

show snmptrap

Syntax Description

show	Display settings.
snmptrap	SNMP trap receivers.

Examples

> **show snmptrap**

SNMP Trap Receiver Name	IP Address	Status
-----	-----	-----
xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	Enable

Related Commands

config snmp version
config snmp trapreceiver

show snmpv3user

To show the SNMP version 3 configuration, use the **show snmpv3user** command.

show snmpv3user

Syntax Description	show	Display settings.
	snmpv3user	SNMP version 3 configuration information.

Examples

```
> show snmpv3user

SNMP v3 User Name      AccessMode Authentication Encryption
-----
default                Read/Write  HMAC-SHA      CFB-AES
```

Related Commands	config snmp version
	config snmp v3user

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	show	Display settings.
	snmpversion	Displays SNMP v1/v2/v3c status (enabled or disabled).

Defaults	Enable.

Examples

```
> show snmpversion
```

```
SNMP v1  Mode..... Disable
SNMP v2c Mode..... Enable
SNMP v3   Mode..... Enable
```

Related Commands	config snmp version

show spanningtree port

To show the Cisco Wireless LAN controller spanning tree port configuration, use the **show spanningtree port** command.

```
show spanningtree port port
```

Syntax Description	show	Display settings.
	spanningtree	Spanning tree.
	port	Displays spanning tree values on a per port basis.
	<i>port</i>	Physical port number: • 1 through 4 on Cisco 2100 series wireless LAN controller. • 1 or 2 on Cisco 4402 series wireless LAN controller. • 1 through 4 on Cisco 4404 series wireless LAN controller.

Defaults 800C, Disabled, 802.1D, 128, 100, Auto.

Usage Guidelines When the a Cisco 4400 Series wireless LAN controller is configured for port redundancy, spanning tree protocol must be disabled for all ports on the Cisco 4400 series wireless LAN controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 series wireless LAN controller.


Note

Some WLAN controllers do not support the spanning tree function.

Examples

```
> show spanningtree port 3

STP Port ID..... 800C
STP Port State..... Disabled
STP Port Administrative Mode..... 802.1D
STP Port Priority..... 128
STP Port Path Cost..... 100
STP Port Path Cost Mode..... Auto
```

Related Commands config spanningtree port

show spanningtree switch

To show the Cisco Wireless LAN controller network (DS port) spanning tree configuration, use the **show spanningtree switch** command.

show spanningtree switch

Syntax Description

show	Display settings.
spanningtree	Spanning tree.
switch	Displays spanning tree values on a per switch basis.



Note

Some WLAN controllers do not support the spanning tree function.

Examples

```
> show spanningtree switch
```

```
STP Specification..... IEEE 802.1D
STP Base MAC Address..... 00:0B:85:02:0D:20
Spanning Tree Algorithm..... Disable
STP Bridge Priority..... 32768
STP Bridge Max. Age (seconds)..... 20
STP Bridge Hello Time (seconds)..... 2
STP Bridge Forward Delay (seconds)..... 15
```

Related Commands

```
config spanningtree switch bridgepriority
config spanningtree switch forwarddelay
config spanningtree switch hellotime
config spanningtree switch maxage
config spanningtree switch mode
```

show stats port

To show physical port receive and transmit statistics, use the **show stats port** command.

show stats port {*detailed port* | *summary port*}

Syntax Description

show	Display settings.
stats	Statistics.
port	Port.
detailed	Displays detailed port statistics.
summary	Displays port summary statistics.
<i>port</i>	Physical port number: • 1 through 4 on Cisco 2100 Series wireless LAN controllers. • 1 or 2 on Cisco 4402 Series wireless LAN controllers. • 1 through 4 on Cisco 4404 Series wireless LAN controllers. • 1 on Cisco WLCM Series wireless LAN controllers.

Examples

```
> show stats port summary 1
```

```
Packets Received Without Error..... 399958
Packets Received With Error..... 0
Broadcast Packets Received..... 8350
Packets Transmitted Without Error..... 106060
Transmit Packets Errors..... 0
Collisions Frames..... 0
Time Since Counters Last Cleared..... 2 day 11 hr 16 min 23 sec
```

```
> show stats port detailed 1
```

```
PACKETS RECEIVED (OCTETS)
Total Bytes..... 267799881
64 byte pkts      :918281
65-127 byte pkts  :354016      128-255 byte pkts  :1283092
256-511 byte pkts :8406        512-1023 byte pkts :3006
1024-1518 byte pkts :1184      1519-1530 byte pkts :0
> 1530 byte pkts   :2

PACKETS RECEIVED SUCCESSFULLY
Total..... 2567987
Unicast Pkts :2547844      Multicast Pkts:0      Broadcast Pkts:20143

PACKETS RECEIVED WITH MAC ERRORS
Total..... 0
Jabbers :0      Undersize :0      Alignment :0
FCS Errors:0      Overruns :0

RECEIVED PACKETS NOT FORWARDED
Total..... 0
Local Traffic Frames:0      RX Pause Frames :0
Unacceptable Frames :0      VLAN Membership :0
VLAN Viable Discards:0      MulticastTree Viable:0
ReserveAddr Discards:0
```



```

CFI Discards           :0                Upstream Threshold :0

PACKETS TRANSMITTED (OCTETS)
Total Bytes..... 353831
64 byte pkts       :0                65-127 byte pkts   :0
128-255 byte pkts  :0                256-511 byte pkts  :0
512-1023 byte pkts :0                1024-1518 byte pkts :2
1519-1530 byte pkts :0                Max Info           :1522

PACKETS TRANSMITTED SUCCESSFULLY
Total..... 5875
Unicast Pkts :5868                Multicast Pkts:0                Broadcast Pkts:7

TRANSMIT ERRORS
Total Errors..... 0
FCS Error       :0                TX Oversized :0                Underrun Error:0

TRANSMIT DISCARDS
Total Discards..... 0
Single Coll Frames :0                Multiple Coll Frames:0
Excessive Coll Frame:0                Port Membership :0
VLAN Viable Discards:0

PROTOCOL STATISTICS
BPDUs Received :6                BPDUs Transmitted :0
802.3x RX PauseFrame:0

Time Since Counters Last Cleared..... 2 day 0 hr 39 min 59 sec

```

Related Commands

config port adminmode

show stats switch

To show the network (DS port) receive and transmit statistics, use the **show stats switch** command.

show stats switch {detailed | summary}

Syntax Description

show	Display settings.
stats	Statistics.
switch	Cisco Wireless LAN controller.
detailed	Displays detailed switch statistics.
summary	Displays switch summary statistics.

Examples

> **show stats switch summary**

```
Packets Received Without Error..... 136410
Broadcast Packets Received..... 18805
Packets Received With Error..... 0
Packets Transmitted Without Error..... 78002
Broadcast Packets Transmitted..... 3340
Transmit Packet Errors..... 2
Address Entries Currently In Use..... 26
VLAN Entries Currently In Use..... 1
Time Since Counters Last Cleared..... 2 day 11 hr 22 min 17 sec
```

> **show stats switch detailed**

```
RECEIVE
Octets..... 19351718
Total Pkts..... 183468
Unicast Pkts..... 180230
Multicast Pkts..... 3219
Broadcast Pkts..... 19
Pkts Discarded..... 0

TRANSMIT
Octets..... 354251
Total Pkts..... 5882
Unicast Pkts..... 5875
Multicast Pkts..... 0
Broadcast Pkts..... 7
Pkts Discarded..... 0

ADDRESS ENTRIES
Most Ever Used..... 1
Currently In Use..... 1

VLAN ENTRIES
Maximum..... 128
Most Ever Used..... 1
Static In Use..... 1
Dynamic In Use..... 0
VLANs Deleted..... 0
Time Since Ctrs Last Cleared..... 2 day 0 hr 43 min 22 sec
```

Related Commands

[config switchconfig mode](#)
[config switchconfig secret-obfuscation](#)
[show switchconfig](#)

show switchconfig

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

show switchconfig

Syntax Description

show	Display settings.
switchconfig	Displays parameters that apply to the Cisco Wireless LAN controller.

Examples

```
> show switchconfig

802.3x Flow Control Mode..... Disable
Current LWAPP Transport Mode..... Layer 3
LWAPP Transport Mode after next switch reboot.... Layer 3
```

Related Commands

- [config switchconfig mode](#)
- [config switchconfig secret-obfuscation](#)
- [show stats switch](#)

show sysinfo

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

show sysinfo

Syntax	Description
show	Display settings.
sysinfo	Cisco Wireless LAN controller information.

Examples

> **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 ap
config country
config sysname
config wlan

Show TACACS Commands

Use the **show tacacs** commands to display Terminal Access Controller Access Control System (TACACS) protocol settings and statistics.

show tacacs acct statistics

This command is used to display detailed RFID information for a specified tag.

show tacacs acct statistics

Syntax Description This command has no arguments or keywords.

Examples

> **show tacacs acct statistics**

Accounting Servers:

```

Server Index..... 1
Server Address..... 10.0.0.0
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 1
Retry Requests..... 0
Accounting Response..... 0
Accounting Request Success..... 0
Accounting Request Failure..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... -1
Timeout Requests..... 1
Unknowntype Msgs..... 0
Other Drops..... 0

```

Related Commands

- config tacacs**
- show tacacs summary**

show tacacs athr statistics

This command is used to display TACACS+ server authorization statistics.

show tacacs athr statistics

Syntax Description This command has no arguments or keywords.

Examples

> **show tacacs athr statistics**

Authorization Servers:

```
Server Index..... 3
Server Address..... 10.0.0.3
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 0
Retry Requests..... 0
Received Responses..... 0
Authorization Success..... 0
Authorization Failure..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Athrenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

Related Commands **config tacacs**
show tacacs summary

show tacacs auth statistics

This command is used to display TACACS+ server authentication statistics.

show tacacs auth statistics

Syntax Description This command has no arguments or keywords.

Examples

```
> show tacacs auth statistics
```

Authentication Servers:

```
Server Index..... 2
Server Address..... 10.0.0.2
Msg Round Trip Time..... 0 (msec)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

Related Commands

- config tacacs
- show tacacs summary

show tacacs summary

This command is used to display TACACS+ server summary information.

show tacacs summary

Syntax Description This command has no arguments or keywords.

Examples

```
> show tacacs summary
```

```
Authentication Servers
```

Idx	Server Address	Port	State	Tout
2	10.0.0.2	6	Enabled	30

```
Accounting Servers
```

Idx	Server Address	Port	State	Tout
1	10.0.0.0	10	Enabled	2

```
Authorization Servers
```

Idx	Server Address	Port	State	Tout
3	10.0.0.3	4	Enabled	2
...				

Related Commands

config tacacs
show tacacs summary

show tech-support

To show Cisco Wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support** command.

show tech-support

Syntax Description

show	Display settings.
tech-support	Displays system resource information.

Examples

```
> 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
```

Related Commands

None.

show time

To show the Cisco Wireless LAN controller time and date, use the **show time** command.

show time

Syntax Description	show	Display settings.
	time	Cisco Wireless LAN controller time and date.

Examples

```
> show time

Time..... Thu Aug  4 19:51:49 2005

Timezone delta..... 0:0
Daylight savings..... disabled

NTP Servers
  NTP Polling Interval.....      86400

  Index      NTP Server
  -----

```

Related Commands	config time

show trapflags

To show the Cisco Wireless LAN controller SNMP trap flags, use the **show trapflags** command.

show trapflags

Syntax	Description
show	Display settings.
trapflags	Displays the Cisco Wireless LAN controller SNMP trap flags.

Examples

```
> 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 Deauthenticate..... Disable
  802.11 Authenticate Failure..... Disable
  802.11 Association Failure..... Disable
  Excluded..... Disable

802.11 Security related traps
  WEP Decrypt Error..... Enable

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

wps..... Enable

configsave..... Enable

IP Security
  esp-auth..... Enable
  esp-replay..... Enable
  invalidSPI..... Enable
  ike-neg..... Enable
  suite-neg..... Enable
```

invalid-cookie..... Enable

Related Commands

config trapflags authentication
config trapflags linkmode
config trapflags multiusers
config trapflags stpmode
config trapflags client
config trapflags ap
config trapflags rrm-profile
config trapflags rrm-params
config trapflags aaa
config trapflags rogueap
config trapflags configsave
config trapflags ipsec
show traplog

show traplog

To show the Cisco Wireless LAN controller SNMP trap log, use the **show traplog** command.

show traplog

Syntax Description

show	Display settings.
traplog	Cisco Wireless LAN controller SNMP trap log.

Examples

```
> 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

show version

This command is used to display access point's software information .

show version

Syntax Description This command has no arguments or keywords.

Usage Guidelines You can only use this command from the access point console port when not connected to a controller.

Examples

```
AP# show version
Cisco IOS Software, C1240 Software (C1240-K9W8-M), Experimental Version
12.3(20060829:081904) [BLD-wnbu_a10_temp_060823.daily 163]
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 30-Aug-06 03:03 by
ROM: Bootstrap program is C1240 boot loader
BOOTLDR: C1240 Boot Loader (C1240-BOOT-M) Version 12.3(7)JA1, RELEASE SOFTWARE (fc1)
Ap1242-2 uptime is 4 minutes
System returned to ROM by power-on
System image file is "flash:/c1240-k9w8-mx.wnbu_a10_temp_060823.20060830d/c1240-k9w8-"
cisco AIR-LAP1242AG-A-K9 processor (revision B0) with 24566K/8192K bytes of memory.
Processor board ID FTX0944B00B
PowerPCelvis CPU at 266Mhz, revision number 0x0950
Last reset from power-on
LWAPP image version 4.1.69.0
1 FastEthernet interface
2 802.11 Radio(s)
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:14:1C:ED:47:14
Part Number : 73-9925-03
PCA Assembly Number : 800-26579-03
PCA Revision Number : A0
PCB Serial Number : FOC09351E0U
Top Assembly Part Number : 800-26804-01
Top Assembly Serial Number : FTX0944B00B
Top Revision Number : A0
Product/Model Number : AIR-LAP1242AG-A-K9
Configuration register is 0xF
```

Related Commands None.

show watchlist

To display the client watchlist, use the **show watchlist** command.

show watchlist

Syntax Description

show	Command action.
watchlist	Displays client watchlist entry.

Examples

```
> show watchlist  
client watchlist state is disabled
```

Related Commands

- config watchlist delete
- config watchlist enable
- config watchlist disable
- config watchlist add

show wlan

To display configuration information for a specified wireless LAN or a foreign access point, or to display wireless LAN summary information, use the **show wlan** command.

show wlan [**apgroups** | **summary** | *wlan_id* | **foreignAp**]

Syntax Description

show	Display settings.
wlan	Wireless LAN.
apgroups	Displays access point group information.
summary	Displays a summary of all wireless LANs.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
foreignAp	Displays the configuration for support of foreign access points.

Examples

```
> show wlan 1
WLAN Identifier..... 1
Profile Name..... wlan
Network Name (SSID)..... wlan
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Admission Control

    NAC-State..... Enabled
    Quarantine VLAN..... 110
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
CHD per WLAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... management
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Allowed
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Peer-to-Peer Blocking Action..... Disabled
Radio Policy..... All
DTIM period for 802.11a radio..... 1
DTIM period for 802.11b radio..... 1
Local EAP Authentication..... Disabled
Security

    802.11 Authentication:..... Open System
    Static WEP Keys..... Disabled
    802.1X..... Disabled
    Wi-Fi Protected Access (WPA/WPA2)..... Enabled
        WPA (SSN IE)..... Disabled
```

```

WPA2 (RSN IE)..... Enabled
  TKIP Cipher..... Disabled
  AES Cipher..... Enabled
Auth Key Managent
  802.1x..... Enabled
  PSK..... Disabled
  CCKM..... Disabled
  FT(802.11r)..... Disabled
FT-PSK(802.11r)..... Disabled
FT Reassociation Timeout..... 20
FT Over-The-Air mode..... Enabled
FT Over-The-Ds mode..... Enabled
CKIP ..... Disabled
IP Security..... Disabled
IP Security Passthru..... Disabled
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Disabled
Auto Anchor..... Disabled
Cranite Passthru..... Disabled
Fortress Passthru..... Disabled
H-REAP Local Switching..... Disabled
Infrastructure MFP protection..... Enabled (Global Infrastructu
MFP Disabled)
  Client MFP..... Optional
  Tkip MIC Countermeasure Hold-down Timer..... 60
Call Snooping..... Enabled

```

```

Mobility Anchor List
WLAN ID      IP Address      Status
-----

```

> **show wlan summary**

```

Number of WLANs..... 2

```

WLAN ID	WLAN Profile Name / SSID	Status	Interface Name
1	test / test	Disabled	management

> **show wlan foreignap**

Foreign AP support is not enabled.

Related Commands

[Configure Wireless LAN Commands](#)
[Configure Wireless LAN Security Commands](#)

Show WPS Commands

Use the **show wps** commands to display Wireless Protection System (WPS) settings.

show wps ap-authentication summary

To display the access point neighbor authentication configuration on the controller, use the **show wps ap-authentication summary** command.

show wps ap-authentication summary

Syntax Description

show	Display settings.
wps	Display WPS settings.
ap-authentication	Access point neighbor authentication settings.
summary	Display the WPS access point neighbor authentication summary.

Examples

```
> show wps ap-authentication summary
```

```
AP neighbor authentication is <disabled>.
```

```
Authentication alarm threshold is 1.
```

```
RF-Network Name: <B1>
```

Related Commands

[config wps ap-authentication](#)

show wps cids-sensor

To display Intrusion Detection System (IDS) sensor summary information or detailed information on a specified Wireless Protection Service (WPS) IDS sensor, use the **show wps cids-sensor detail** command.

show wps cids-sensor { **summary** | **detail** *index* }

Syntax Description

show	Display settings.
wps	Wireless Protection Service settings.
cids-sensor	IDS sensor settings.
summary	Show a summary of sensor settings.
detail	Display all settings for the selected sensor.
<i>index</i>	IDS sensor identifier.

Examples

```
> show wps cids-sensor detail 1
```

```
IP Address..... 10.0.0.51
Port..... 443
Query Interval..... 60
Username..... Sensor_user1
Cert Fingerprint..... SHA1: 00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00
Query State..... Disabled
Last Query Result..... Unknown
Number of Queries Sent..... 0
```

Related Commands

[config wps cids-sensor](#)

show wps mfp

To display Management Frame Protection (MFP) information, use the **show wps mfp** command.

show wps mfp {summary | statistics}

Syntax Description

show	Command action.
wps	Displays WPS configuration.
mfp	Displays Management Frame Protection information.
summary	Displays MFP configuration and status.
statistics	Displays MFP statistics.

Examples

> **show wps mfp summary**

```
Global Infrastructure MFP state..... DISABLED (*all infrastructure
settings are overridden)
Controller Time Source Valid..... False
```

WLAN ID	WLAN Name	WLAN Status	Infra. Protection	Client Protection
1	homeap (WPA2 not configured)	Disabled	*Enabled	Optional but inactive
2	7921 (WPA2 not configured)	Enabled	*Enabled	Optional but inactive
3	open1 (WPA2 not configured)	Enabled	*Enabled	Optional but inactive
4	7920 (WPA2 not configured)	Enabled	*Enabled	Optional but inactive

AP Name	Infra. Validation	Radio	Operational State	--Infra. Capability-- Protection	Validation
AP1252AG-EW	*Enabled	b/g	Down	Full	Full
		a	Down	Full	Full

>**show wps mfp statistics**

BSSID	Radio Validator	AP	Last Source Addr	Found	Error Type
Count	Frame Types				
no errors					

Related Commands

[config wps mfp](#)

show wps shun-list

To display Intrusion Detection System (IDS) sensor shun list, use the **show wps shun-list** command.

show wps shun-list

Syntax Description	This command has no arguments or keywords.

Examples	> show wps shun-list

Related Commands	config wps shun-list

show wps signature detail

To display installed signatures, use the **show wps signature detail** command.

show wps signature detail *sig-id*

Syntax Description

show	Display settings.
wps	Wireless Protection System settings.
signature	Installed signature settings.
detail	Display all signature settings for the selected signature.
<i>sig-id</i>	A signature ID of an installed signature.

Examples

To display information on the attacks detected by standard signature 1, use this command:

```
>show wps signature detail 1
```

```
Signature-ID..... 1
Precedence..... 1
Signature Name..... Bcast deauth
Type..... standard
FrameType..... management
State..... enabled
Action..... report
Tracking..... per Signature and Mac
Signature Frequency..... 500 pkts/interval
Signature Mac Frequency..... 300 pkts/interval
Interval..... 10 sec
Quiet Time..... 300 sec
Description..... Broadcast Deauthentication Frame
Patterns:
    0 (Header) : 0x0:0x0
    4 (Header) : 0x0:0x0
```

Related Commands

[config wps signature](#)
[config wps signature frequency](#)
[config wps signature interval](#)
[config wps signature mac-frequency](#)
[config wps signature quiet-time](#)
[config wps signature reset](#)
[show wps signature summary](#)
[show wps summary](#)

show wps signature events

To display more information on the attacks detected by a particular standard or custom signature, use the **show wps signature events** command.

show wps signature events {**summary** | {**standard** | **custom**} *precedenceID* {**summary** | **detailed**}}

Syntax Description

show	Display settings.
wps	Wireless Protection Service settings.
summary	Display all tracking signature summary information.
standard	Standard Intrusion Detection System (IDS) signature settings.
custom	Custom IDS signature settings.
<i>precedenceID</i>	Signature precedence identification value.
summary detailed	- Enter summary to display a tracking signature summary. - Enter detailed to display tracking source MAC address details.

Examples

To display the number of attacks detected by all enabled signatures, enter this command:

```
> show wps signature events summary
```

Precedence	Signature Name	Type	# Events
1	Bcast deauth	Standard	2
2	NULL probe resp 1	Standard	1

To display a summary of information on the attacks detected by standard signature 1, enter this command:

```
> show wps signature events standard 1 summary
```

```
Precedence..... 1
Signature Name..... Bcast deauth
Type..... Standard
Number of active events..... 2
```

Source MAC Addr	Track Method	Frequency	# Aps	Last Heard
00:a0:f8:58:60:dd	Per Signature	50	1	Wed Oct 25 15:03:05 2006
00:a0:f8:58:60:dd	Per Mac	30	1	Wed Oct 25 15:02:53 2006

Related Commands

[config wps signature](#)
[config wps signature frequency](#)
[config wps signature interval](#)
[config wps signature mac-frequency](#)
[config wps signature quiet-time](#)
[config wps signature reset](#)
[show wps signature summary](#)
[show wps summary](#)

show wps signature summary

To see individual summaries of all of the standard and custom signatures installed on the controller, use the **show wps signature summary** command.

show wps signature summary

Syntax Description This command has no arguments or keywords.

Examples

```
> show wps signature summary

Signature-ID..... 1
Precedence..... 1
Signature Name..... Bcast deauth
Type..... standard
FrameType..... management
State..... enabled
Action..... report
Tracking..... per Signature and Mac
Signature Frequency..... 50 pkts/interval
Signature Mac Frequency..... 30 pkts/interval
Interval..... 1 sec
Quiet Time..... 300 sec
Description..... Broadcast Deauthentication Frame
Patterns:
    0 (Header) : 0x00c0:0x00ff
    4 (Header) : 0x01:0x01
...
```

Related Commands

- [config wps signature](#)
- [config wps signature frequency](#)
- [config wps signature interval](#)
- [config wps signature mac-frequency](#)
- [config wps signature quiet-time](#)
- [config wps signature reset](#)
- [show wps signature events](#)
- [show wps summary](#)

show wps summary

To display WPS summary information, use the **show wps summary** command.

show wps summary

Syntax Description

This command has no arguments or keywords.

Examples

> **show wps summary**

```
Auto-Immune
  Auto-Immune..... Disabled

Client Exclusion Policy
  Excessive 802.11-association failures..... Enabled
  Excessive 802.11-authentication failures..... Enabled
  Excessive 802.1x-authentication..... Enabled
  IP-theft..... Enabled
  Excessive Web authentication failure.....Enabled

Trusted AP Policy
  Management Frame Protection..... Disabled
  Mis-configured AP Action..... Alarm Only
    Enforced encryption policy..... none
    Enforced preamble policy..... none
    Enforced radio type policy..... none
  Validate SSID..... Disabled
  Alert if Trusted AP is missing..... Disabled
  Trusted AP timeout..... 120

Untrusted AP Policy
  Rogue Location Discovery Protocol..... Disabled
  RLDP Action..... Alarm Only
  Rogue APs
    Rogues AP advertising my SSID..... Alarm Only
    Detect and report Ad-Hoc Networks..... Enabled
  Rogue Clients
    Validate rogue clients against AAA..... Enabled
    Detect trusted clients on rogue APs..... Alarm Only
  Rogue AP timeout..... 1300

Signature Policy
  Signature Processing..... Enabled
...
```

Related Commands

[config wps signature](#)
[config wps signature frequency](#)
[config wps signature interval](#)
[config wps signature mac-frequency](#)
[config wps signature quiet-time](#)
[config wps signature reset](#)
[show wps signature events](#)
[show wps signature summary](#)

show wps wips statistics

To display the current state of Cisco wireless intrusion prevention system (wIPS) operation on the controller, use the **show wps wips summary** command.

show wps wips statistics

Syntax Description This command has no arguments or keywords.

Examples

```
> show wps wips statistics

Policy Assignment Requests..... 1
Policy Assignment Responses..... 1
Policy Update Requests..... 0
Policy Update Responses..... 0
Policy Delete Requests..... 0
Policy Delete Responses..... 0
Alarm Updates..... 13572
Device Updates..... 8376
Device Update Requests..... 0
Device Update Responses..... 0
Forensic Updates..... 1001
Invalid WIPS Payloads..... 0
Invalid Messages Received..... 0
NMSP Transmitted Packets..... 22950
NMSP Transmit Packets Dropped..... 0
NMSP Largest Packet..... 1377
```

Related Commands

- [config 802.11 enable](#)
- [config ap mode](#)
- [config ap monitor-mode](#)
- [show ap config](#)
- [show ap monitor-mode summary](#)
- [show wps wips summary](#)

show wps wips summary

To display Cisco wireless intrusion prevention system (wIPS) configuration forwarded by WCS to the controller, use the **show wps wips summary** command.

show wps wips summary

Syntax Description	This command has no arguments or keywords.

Examples

```
> show wps wips summary
```

```
Policy Name..... Default
Policy Version..... 3
```

Related Commands

[config 802.11 enable](#)
[config ap mode](#)
[config ap monitor-mode](#)
[show ap config](#)
[show ap monitor-mode summary](#)
[show wps wips statistics](#)

Configuring Controller Settings

Use the **config** commands to configure Cisco Wireless LAN (WLAN) controller options and settings.

Configure 802.11 Network Commands

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

Configure 802.11 Public Safety Commands

Use the **config 802.11-a** commands to configure settings specifically for 4.9 GHz or 5.8 GHz Public safety frequencies.

config 802.11-a

To enable or disable the public safety channels 4.9-GHz and 5.8-GHz on an access point, use the **config 802.11-a** commands.

```
config {802.11-a49 | 802.11-a58} {enable | disable} cisco_ap
```

Syntax Description

config	Configuration settings.
802.11-a49 802.11-a58	- Enter 802.11-a49 to select the 4.9-GHz public safety channel. - Enter 802.11-a58 to select the 5.8-GHz public safety channel.
enable disable	Enable or disable the use of this frequency on the designated access point
cisco_ap	The name of the access point to which the command applies.

Command Default

Disabled.

Examples

To enable the public safety channel *4.9-GHz* on *ap_24* access point, enter this command:

```
> config 802.11-a49 enable ap_24
```

Related Commands

- [config 802.11-a antenna extAntGain](#)
- [config 802.11-a channel ap](#)
- [config 802.11-a txpower ap](#)
- [show 802.11](#)
- [show mesh public-safety](#)

config 802.11-a antenna extAntGain

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

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

Syntax Description	
config	Configuration settings.
802.11-a49 802.11-a58	- Enter 802.11-a49 to select the 4.9-GHz public safety channel. - Enter 802.11-a58 to select the 5.8-GHz public safety channel.
antenna	Access point antenna settings.
extAntGain	External antenna gain settings for public safety channels.
<i>ant_gain</i>	A value in .5-dBi units (for instance, 2.5 dBi = 5)
<i>cisco_ap</i>	The name of the access point to which the command applies.
global channel_no	- Enter global to apply the antenna gain value to all channels. - Enter <i>channel_no</i> to apply the antenna gain value to a specific channel.

Command Default Disabled.

Usage Guidelines

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

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

Examples

To configure an *802.11-a49* external antenna gain of 5 dBi for *AP1*:

```
> config 802.11-a49 antenna extAntGain 10 AP1
```

Related Commands

[config 802.11-a](#)
[config 802.11-a channel ap](#)
[config 802.11-a txpower ap](#)
[show 802.11](#)

config 802.11-a channel ap

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

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

Syntax Description	config	Configuration settings.
	802.11-a49 802.11-a58	- Enter 802.11-a49 to select the 4.9-GHz public safety channel. - Enter 802.11-a58 to select the 5.8-GHz public safety channel.
	channel	Configure channel settings.
	ap	Configure access point channel settings.
	<i>cisco_ap</i>	The name of the access point to which the command applies.
	global channel_no	- Enter global to enable dynamic channel assignment (RRM) on all 4.9-GHz and 5.8-GHz subband radios. - Enter <i>channel_no</i> to set a custom channel for a specific mesh access point. Valid range is 1 through 26, inclusive for 4.9-GHz band and 149 through 165, inclusive for 5.8-GHz band.

Command Default Disabled.

Examples To set the channel

```
> config 802.11-a49 channel ap
```

Related Commands

[config 802.11-a](#)
[config 802.11-a antenna extAntGain](#)
[config 802.11-a channel ap](#)
[config 802.11-a txpower ap](#)
[show 802.11](#)

config 802.11-a txpower ap

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

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

Syntax Description	
config	Configuration settings.
802.11-a49 802.11-a58	- Enter 802.11-a49 to select the 4.9-GHz public safety channel. - Enter 802.11-a58 to select the 5.8-GHz public safety channel.
channel	Configure channel settings.
ap	Configure access point channel settings.
<i>cisco_ap</i>	The name of the access point to which the command applies.
global <i>power_level</i>	- Enter global to apply the transmission power value to all channels. - Enter <i>power_level</i> to apply the transmission power value to the designated mesh access point. Valid values are: 1-5, inclusive.

Command Default Disabled.

Examples To configure an *802.11-a49* transmission power level of *4* for *AP1*:

```
> config 802.11-a49 txpower ap 4 AP1
```

Related Commands

- [config 802.11-a](#)
- [config 802.11-a antenna extAntGain](#)
- [config 802.11-a channel ap](#)
- [show 802.11](#)

Configure 802.11b Commands

Use the **config 802.11b** commands to configure settings specifically for an 802.11b/g network.

config 802.11b 11gSupport

To enable or disable the Cisco wireless LAN solution 802.11g network, use the **config 802.11b 11gSupport** command:

config 802.11b 11gSupport {enable | disable}



Note See Usage Guidelines before using this command.

Syntax Description

config	Configuration settings.
802.11b	802.11b network settings.
11gSupport	Support for the 802.11g network.
enable disable	Enable or disable 802.11g.

Defaults

Enabled.

Usage Guidelines

This command enables the Cisco wireless LAN solution 802.11g network *after* the Cisco wireless LAN solution 802.11b network is enabled using the [config 802.11 enable](#) command.

You must use this command to enable the network after configuring other 802.11b parameters. This command can be used any time the CLI interface is active.



Note To disable an 802.11a, 802.11b and/or 802.11g network for an individual wireless LAN, use the **config wlan radio** command.

Examples

```
> config 802.11b 11gSupport enable
```

```
Changing the 11gSupport will cause all the APs to reboot when you enable 802.11b network.
Are you sure you want to continue? (y/n) n
```

```
11gSupport not changed!
```

Related Commands

```
show sysinfo
show 802.11b
config 802.11b enable
config wlan radio
config 802.11b disable
config 802.11a disable
config 802.11a enable
```

config 802.11b preamble

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

config 802.11b preamble {long | short}

Syntax Description	config	Configuration settings.
	802.11b	802.11b network parameters.
	preamble	As defined in subclause 18.2.2.2.
	{long short}	Long or short 802.11b preamble.

Defaults Short.



Usage Guidelines **Note** You must reboot the Cisco Wireless LAN controller (reset system) with save to implement this command.

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

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

Examples

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

> show 802.11b
Short Preamble mandatory..... Enabled

> config 802.11b preamble long
>(reset system with save)

> show 802.11b
Short Preamble mandatory..... Disabled
```

Related Commands show 802.11b

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

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

Syntax Description	config	Configuration settings.
	802.11h	802.11h network settings.
	channelswitch	802.11h channel switch announcement.
	enable disable	Enable or disable 802.11h channel switch announcement.
	mode	802.11h channel switch announcement mode.
	value	802.11h channel announcement value.

Defaults	None.

Examples	> config 802.11h channelswitch disable

Related Commands	show 802.11h

config 802.11h powerconstraint

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

config 802.11h powerconstraint *value*

Syntax Description	config	Configuration settings.
	802.11h	802.11h network settings.
	powerconstraint	Configure power constraint settings.
	<i>value</i>	802.11h power constraint value.

Defaults	None.

Examples	> 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	config	Configuration settings.
	802.11h	802.11h network settings.
	setchannel	Channel configuration settings.
	cisco_ap	Cisco lightweight access point name.

Defaults None.

Examples > config 802.11h setchannel ap02

Related Commands show 802.11h

Configure 802.11 11n Support Commands

Use the **config 802.11 11nsupport** 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	config	Configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	11nsupport	Support for 802.11n devices.
	enable disable	Enable or disable 802.11n support.

Defaults None.

Examples `> 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 }
```



Note 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.

Syntax Description

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
11nsupport	Support for 802.11n devices.
a-mpdu tx priority	Aggregated MAC Protocol Data Unit priority levels assigned per traffic type: • 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.
enable	The traffic associated with the priority level uses A-MPDU transmission.
disable	The traffic associated with the priority level uses A-MSDU transmission.

Defaults

All priorities, except 5 and 6, are enabled by default. Priorities 5 and 6 are disabled by default.

Examples

```
> 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 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 {tx | rx} cisco_ap {A | B | C} {enable | disable}
```

Syntax Description	config	Configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	11nsupport antenna	Support for 802.11n devices.
	tx	Enable the antenna to transmit.
	rx	Enable the antenna to receive.
	cisco_ap	Specify the access point.
	A B C	The antenna ports. A is the right antenna port, B is the left antenna port, and C is the center antenna port.
	enable disable	Enable or disable this configuration.

Defaults None.

Examples config 802.11a 11nsupport antenna tx 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 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
config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
11n support	Support for 802.11n devices.
mcs tx	Modulation and coding scheme data rates: • 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 disable	Enable or disable this configuration.

Defaults None.

Examples

```
> config 802.11a 11n support mcs tx 5 enable
```

Related Commands

- config 802.11 11n support
- config wlan wmm required
- config 802.11 11n support 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
```

Configure 802.11 Antenna Commands

Use the config 802.11 antenna commands to configure radio antenna settings for Cisco Lightweight access points on different 802.11 networks.

config 802.11 antenna diversity

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

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

Syntax Description		
config		Configuration settings.
802.11		802.11 network settings.
a b		Specifies 802.11a or 802.11b/g network.
antenna diversity		Configure antenna diversity settings.
enable		Between the two internal antennas.
sideA		Between the internal antennas and an external antenna connected to the Cisco lightweight access point left port.
sideB		Between the internal antennas and an external antenna connected to the Cisco lightweight access point right port.
<i>cisco_ap</i>		Cisco lightweight access point name.

Defaults None.

Examples

To enable antenna diversity for AP01 on an 802.11b network, enter this command:

```
> config 802.11b antenna diversity enable AP01
```

To enable diversity for AP01 on an 802.11a network, using an external antenna connected to the Cisco lightweight access point Left port (sideA), enter this command:

```
> config 802.11a antenna diversity sideA AP01
```

Related Commands

- [config 802.11 disable](#)
- [config 802.11 enable](#)
- [config 802.11 antenna extAntGain](#)
- [config 802.11 antenna mode](#)
- [config 802.11 antenna selection](#)
- [show 802.11](#)

config 802.11 antenna extAntGain

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

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

Syntax Description	config	Configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	antenna	Configure antenna settings.
	extAntGain	Configure external antenna gain.
	antenna_gain	Enter antenna gain in 0.5 dBm units (for example, 2.5 dBm = 5).
	cisco_ap	Cisco lightweight access point name.

Defaults None.

Usage Guidelines

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

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

Examples

To configure an *802.11a* external antenna gain of *0.5 dBm* for *AP1*:

```
> config 802.11a antenna extAntGain 1 AP1
```

Related Commands

- config 802.11 disable
- config 802.11 enable
- config 802.11 antenna diversity
- config 802.11 antenna mode
- config 802.11 antenna selection
- show 802.11

config 802.11 antenna mode

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

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

Syntax Description		
config		Configuration settings.
802.11		802.11 network settings.
a b		Specifies 802.11a or 802.11b/g network.
antenna mode		Configure antenna coverage pattern settings.
omni		Use both internal antennas.
sectorA		Use only the Side A internal antenna.
sectorB		Use only the Side B internal antenna.
<i>cisco_ap</i>		Cisco lightweight access point name.

Defaults None.

Examples To configure access point AP01 antennas for a 360-degree omnidirectional pattern on an 802.11b network, enter this command:

```
> config 802.11b antenna mode omni AP01
```

Related Commands

- [config 802.11 disable](#)
- [config 802.11 enable](#)
- [config 802.11 antenna diversity](#)
- [config 802.11 antenna extAntGain](#)
- [config 802.11 antenna selection](#)
- [show 802.11](#)

config 802.11 antenna selection

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

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

Syntax Description	config	Configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	antenna selection	Select antenna type.
	internal external	Select internal or external antenna.
	cisco_ap	Cisco lightweight access point name.

Defaults None.

Examples To configure access point AP02 on an 802.11b network to use it's internal antenna, enter this command:
> config 802.11b antenna selection internal AP02

Related Commands

- config 802.11 disable
- config 802.11 enable
- config 802.11 antenna diversity
- config 802.11 antenna extAntGain
- config 802.11 antenna mode
- config 802.11 antenna selection
- show 802.11

config 802.11 beaconperiod

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

config 802.11{a | b} beaconperiod *time_units*



Note

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

Syntax Description

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
beaconperiod	Send a beacon every 20 to 1000 milliseconds.
<i>time_units</i>	Beacon interval in time units (TU). One TU is 1024 micro seconds.

Defaults

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 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 using the **config 802.11 disable** command. After changing the beacon period, enable the 802.11 network using the **config 802.11 enable** command.

Examples

To configure an 802.11a network for a beacon period of 120 time units, enter this command:

```
> config 802.11a beaconperiod 120
```

Related Commands

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

config 802.11 beamforming

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

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



Note

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

Syntax Description

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
beamforming	Configure beamforming.
global	All lightweight access points.
ap <i>ap_name</i>	Cisco access point name.
enable disable	Enable or disable beamforming.

Defaults

None.

Usage Guidelines

Follow these guidelines for using beamforming:

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



Note

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

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

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

Examples

To configure an 802.11a network for a beacon period of 120 time units, enter this command:

```
> config 802.11a beamforming global enable
> config 802.11a beamforming ap 1250-1 disable
```

Related Commands

- show ap config {802.11a | 802.11b}
- show 802.11a
- config 802.11b beaconperiod
- config 802.11a disable
- config 802.11a enable

Configure 802.11 CAC Commands

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

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

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
cac	Call Admission Control settings.
video	Video traffic settings.
acm	Admission Control Management for video settings.
enable disable	Enable or disable video CAC.

Defaults

Disabled.

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: **config wlan disable wlan_id**
- Disable the radio network you wish to configure: **config 802.11{a | b} disable network**
- Save the new configuration: **save config**
- Enable voice or video CAC for the network you wish to configure:
config 802.11{a | b} cac voice acm enable, or
config 802.11{a | b} cac video acm enable

For complete instructions, refer to 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

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

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
cac	Call Admission Control parameters.
video	Video traffic parameters.
max-bandwidth	Specify the percentage of the maximum allocated bandwidth for video applications on the selected radio band.
<i>bandwidth</i>	A bandwidth percentage value from 0-100%.

Defaults

0%

Usage Guidelines

The maximum radio frequency (RF) bandwidth cannot exceed 100% for voice + 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 the operator does not want to allocate any bandwidth and therefore allows all bandwidth requests.

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: **config wlan disable** *wlan_id*
- Disable the radio network you wish to configure: **config 802.11{a | b} disable network**
- Save the new configuration: **save config**
- Enable voice or video CAC for the network you wish to configure:
config 802.11{a | b} cac voice acm enable, or
config 802.11{a | b} cac video acm enable

For complete instructions, refer to 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

```
> config 802.11a cac video max-bandwidth 50
> config 802.11b cac video max-bandwidth 75
```

Related Commands

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

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

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
cac	Call Admission Control parameters.
video	Video traffic parameters.
roam-bandwidth	Specify the percentage of the maximum allocated bandwidth reserved for roaming video clients on the selected radio band.
<i>bandwidth</i>	A bandwidth percentage value from 0 to 25%.

Defaults

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 the operator does not want to do any bandwidth allocation and, therefore, allows all bandwidth requests.

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: **config wlan disable** *wlan_id*
- Disable the radio network you wish to configure: **config 802.11{a | b} disable network**
- Save the new configuration: **save config**
- Enable voice or video CAC for the network you wish to configure:
config 802.11{a | b} cac voice acm enable, or
config 802.11{a | b} cac video acm enable

For complete instructions, refer to 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

```
> config 802.11a cac video roam-bandwidth 10
> config 802.11b cac video roam-bandwidth 0
```

Related Commands

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

config 802.11 cac video tspec-inactivity-timeout

To process or ignore the 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

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
cac	Call Admission Control parameters.
video	Video traffic parameters.
tspec-inactivity-timeout	Specify the response to TSPEC inactivity timeout messages received from an access point.
enable ignore	Process or ignore the TSPEC inactivity timeout messages.

Defaults

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: **config wlan disable wlan_id**
- Disable the radio network you wish to configure: **config 802.11{a | b} disable network**
- Save the new configuration: **save config**
- Enable voice or video CAC for the network you wish to configure:
config 802.11{a | b} cac voice acm enable, or
config 802.11{a | b} cac video acm enable

For complete instructions, refer to 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

```
> config 802.11a cac video tspec-inactivity-timeout enable
> config 802.11b 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

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
cac	Call Admission Control parameters.
voice	Voice traffic parameters.
acm	Admission control.
enable disable	Enable or disable bandwidth-based CAC.

Defaults

Disabled.

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: **config wlan disable wlan_id**
- Disable the radio network you wish to configure: **config 802.11 {a | b} disable network**
- Save the new configuration: **save config**
- Enable voice or video CAC for the network you wish to configure:
config 802.11 {a | b} cac voice acm enable, or
config 802.11 {a | b} cac video acm enable

For complete instructions, refer to 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

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

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
cac	Call Admission Control parameters.
voice	Voice traffic parameters.
max-bandwidth	Specify the percentage of the maximum allocated bandwidth for voice applications on the selected radio band.
<i>bandwidth</i>	A bandwidth percentage value from 40-85%.

Defaults

75%

Usage Guidelines

The maximum radio frequency (RF) bandwidth cannot exceed 100% for voice + video. Once the client reaches the value specified, the access point rejects new calls on this network.

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: **config wlan disable** *wlan_id*
- Disable the radio network you wish to configure: **config 802.11{a | b} disable network**
- Save the new configuration: **save config**
- Enable voice or video CAC for the network you wish to configure:
config 802.11{a | b} cac voice acm enable, or
config 802.11{a | b} cac video acm enable

For complete instructions, refer to 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

```
> config 802.11a cac voice max-bandwidth 50
> config 802.11b cac voice max-bandwidth 75
```

Related Commands

```
config 802.11 cac voice acm
config 802.11 cac voice load-based
config 802.11 cac voice roam-bandwidth
```

```
config 802.11 cac voice stream-size
config 802.11 cac voice tspec-inactivity-timeout
config 802.11 exp-bwreq
config 802.11 tsm
config wlan {enable | disable}
save config
show wlan
show wlan summary
```

config 802.11 cac voice roam-bandwidth

To configure the percentage of the 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	config	Configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	cac	Call Admission Control parameters.
	voice	Voice traffic parameters.
	roam-bandwidth	Specify the percentage of the maximum allocated bandwidth reserved for roaming voice clients on the selected radio band.
	bandwidth	A bandwidth percentage value from 0 to 25%.

Defaults

6%

Usage Guidelines

The maximum radio frequency (RF) bandwidth cannot exceed 100% for voice + 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 that the operator does not want to allocate any bandwidth and therefore allows all bandwidth requests.

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: **config wlan disable** *wlan_id*
- Disable the radio network you wish to configure: **config 802.11{a | b} disable network**
- Save the new configuration: **save config**
- Enable voice or video CAC for the network you wish to configure:
config 802.11{a | b} cac voice acm enable, or
config 802.11{a | b} cac video acm enable

For complete instructions, refer to 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

```
> config 802.11a cac voice roam-bandwidth 10
> config 802.11b cac voice roam-bandwidth 6
```

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 stream-size,
config 802.11 cac voice tspec-inactivity-timeout,

config 802.11 cac voice tspec-inactivity-timeout

To process or ignore the 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

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
cac	Call Admission Control parameters.
voice	Voice traffic parameters.
tspec-inactivity-timeout	Specify the response to TSPEC inactivity timeout messages received from an access point.
enable ignore	Process or ignore the TSPEC inactivity timeout messages.

Defaults

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: **config wlan disable wlan_id**
- Disable the radio network you wish to configure: **config 802.11{a | b} disable network**
- Save the new configuration: **save config**
- Enable voice or video CAC for the network you wish to configure:
config 802.11{a | b} cac voice acm enable, or
config 802.11{a | b} cac video acm enable

For complete instructions, refer to 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

```
> config 802.11a cac voice tspec-inactivity-timeout enable
> config 802.11b cac voice tspec-inactivity-timeout ignore
```

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 stream-size
```

config 802.11 cac voice load-based

To enable or disable load-based 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

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
cac	Call Admission Control parameters.
voice	Voice traffic parameters.
load-based	Load-based CAC parameters.
enable disable	Enable or disable load-based CAC.

Defaults

Disabled.

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: **config wlan disable wlan_id**
- Disable the radio network you wish to configure: **config 802.11 {a | b} disable network**
- Save the new configuration: **save config**
- Enable voice or video CAC for the network you wish to configure:
config 802.11 {a | b} cac voice acm enable, or
config 802.11 {a | b} cac video acm enable

For complete instructions, refer to 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

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

Related Commands

config 802.11 cac voice acm
config 802.11 cac voice max-bandwidth
config 802.11 cac voice roam-bandwidth
config 802.11 cac voice stream-size
config 802.11 cac voice tspec-inactivity-timeout

config 802.11 cac voice stream-size

To configure the number of aggregated voice 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 *number max-streams mean_datarate*

Syntax Description		
config		Configuration settings.
802.11		802.11 network settings.
a b		Specifies 802.11a or 802.11b/g network.
cac		Call Admission Control parameters.
voice		Voice traffic parameters.
stream-size		Configures the number of voice streams that the controller supports.
<i>number</i>		Specifies the number (1 to 5) of voice streams.
max-streams		Configures the mean data rate of a voice stream.
<i>mean_datarate</i>		Specifies the mean data rate (84 to 91.2 Kbps) of a voice stream.

Defaults

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 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: **config wlan disable wlan_id**
- Disable the radio network you wish to configure: **config 802.11{a | b} disable network**
- Save the new configuration: **save config**
- Enable voice or video CAC for the network you wish to configure:
config 802.11{a | b} cac voice acm enable, or
config 802.11{a | b} cac video acm enable

For complete instructions, refer to 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

```
> config 802.11a cac voice stream-size 5 max-streams size 85
> config 802.11b cac voice stream-size 3 max-streams size 90
```

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 channel

To configure an 802.11 network or a single access point for automatic or manual channel selection, use the **config 802.11 channel** command.

config 802.11{a | b} **channel** {global [auto | once | off]} | {AP ap_name [global | channel]}

Syntax Description	
config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
channel	
auto	Specifies the channel is automatically set by radio resource management (RRM) for the 802.11a radio.
once	Specifies the channel is automatically set once by RRM.
off	Specifies the automatic channel selection by RRM is disabled.
ap	Configures the 802.11a operating channel for a specified lightweight access point.
<i>ap_name</i>	Specifies the access point name.
global	Specifies the 802.11a operating channel is automatically set by RRM and over-rides the existing configuration setting.
<i>channel</i>	Specifies a manual channel number to be used by the access point. The supported channels depend on the specific access point used and the regulatory region.

Defaults None.

Usage Guidelines When configuring 802.11 channels for a single lightweight access point, use the **config 802.11 disable** command to disable the 802.11 network. Then use the **config 802.11 channel** command to set automatic channel selection by Radio Resource Management (RRM) or manually set the channel for the 802.11 radio. Then enable the 802.11 network using the **config 802.11 enable** command.



Note Refer to the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the channels supported by your access point. The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

Examples To configure all 802.11a channels for automatic channel configuration by the RRM based on availability and interference, enter this command:

```
> config 802.11a channel global auto
```

To have RRM automatically reconfigure all 802.11b channels one time based on availability and interference, enter this command:

```
> config 802.11b channel global once
```

To turn 802.11a automatic channel configuration off, enter this command:

```
> config 802.11a channel global off
```

To configure all 802.11b channels in access point AP01 for automatic channel configuration, enter this command:

```
> config 802.11b channel AP01 global
```

To configure 802.11a channel 36 in access point AP01 as the default channel, enter this command:

```
> config 802.11a channel AP01 36
```

Related Commands

```
show 802.11a
config 802.11a disable
config 802.11a enable
config 802.11b channel
config country
```

config 802.11 channel ap

To set the operating radio channel for an access point, use the **config 802.11 channel ap** command.

```
config 802.11{a | b} channel ap cisco_ap {global | channel_no}
```

Syntax Description		
config		Configuration settings.
802.11		802.11 network settings.
a b		Specifies 802.11a or 802.11b/g network.
channel		Radio channel settings for an 802.11 network.
ap		Configures the operating channel for a specified lightweight access point.
<i>cisco_ap</i>		The name of the Cisco access point.
global		Enable auto-RF on the designated access point.
<i>channel_no</i>		Specifies the default channel from 1 to 26, inclusive.

Defaults	None.

Examples	To enable auto-RF for access point AP01 on an 802.11b network, enter this command: > config 802.11b channel ap ap01 global

Related Commands	show 802.11a config 802.11b channel config country

config 802.11 chan_width

To configure the channel width for a particular access point, enter this command:

```
config 802.11 {a | b} chan_width cisco_ap {20 | 40}
```

Syntax Description		
config		Configuration settings.
802.11		802.11 network settings.
a b		Specifies 802.11a or 802.11b/g network.
chan_width		The channel width for a particular access point
<i>cisco_ap</i>		Specify the access point.
20		Allows the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels.
40		Allows 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together.

Defaults

Default channel width is **20**.

Usage Guidelines

This parameter can be configured only if the primary channel is statically assigned.

Cisco recommends that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference can occur.

Statically configuring an access point's radio for 20- or 40-MHz mode overrides the globally configured DCA channel width setting (configured using the [config advanced 802.11 channel dca chan-width-11n](#) command). If you ever change the static configuration back to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

Examples

```
> config 802.11a chan_width cisco_ap 40
```

Related Commands

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

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		
config		Configuration settings.
802.11		802.11 network settings.
a b		Specifies 802.11a or 802.11b/g network.
disable		Disables 802.11 transmission.
network		Disables transmission for the entire 802.11a network.
<i>cisco_ap</i>		Disables transmission for an individual Cisco lightweight access point radio.

Defaults

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 the CLI interface is active.

Examples

To disable the entire 802.11a network:

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

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	config	Configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	dtpc	Configure DTPC settings.
	enable disable	Enable or disable support for this command.

Defaults Enabled by default.

Examples To disable DTPC for an 802.11a network, enter this command:
> 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	config	Configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	enable	Disables 802.11 transmission.
	network	Disables transmission for the entire 802.11a network.
	<i>cisco_ap</i>	Disables transmission for an individual Cisco lightweight access point radio.

Defaults 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 the CLI interface is active.

Examples To enable radio transmission for the entire 802.11a network, enter this command:

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

To enable radio transmission for AP1 on a 802.11b network, enter this command:

```
> 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 CCX version 5 expedited bandwidth request feature for an 802.11 radio, use the **config 802.11 exp-bwreq** command. When this command is enabled, the controller configures all joining access points for this feature.

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

Syntax Description	config	Configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	exp-bwreq	CCX expedited bandwidth settings.
	enable disable	Enables the expedited bandwidth request feature.
	disable	Configures the mean datarate of a voice stream.

Defaults The expedited bandwidth request feature is disabled by default.

Examples

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

Cannot change Exp Bw Req mode while 802.11a network is operational.

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

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	config	Configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	fragmentation	Fragmentation threshold.
	<i>threshold</i>	A number between 256 and 2346 bytes (inclusive)

Defaults None.

Examples > **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, enter this command:

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

Syntax Description

config	Configuration settings.
802.11	802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
l2roam	Support for Layer 2 client roaming.
rf-params	Radio frequency parameters.
default	Restores Layer 2 client roaming RF parameters to default values.
custom	Configures custom Layer 2 client roaming RF parameters.
<i>min_rssi</i>	The 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. Therefore, 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>	The hysteresis value indicates 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>	The scan threshold value is the 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>	The transition time is the 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, Cisco recommends that you set the transition time to 1 second.

Defaults

<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, Cisco recommends that you set the *trans_time* to 1 second.

Examples

```
> config 802.11a l2roam rf-params custom -80 2 -70 7
```

Related Commands

[show advanced 802.11 l2roam](#)
[show l2tp](#)

config 802.11 pico-cell

To enable or disable the 802.11 pico-cell extensions, use the **config 802.11 pico-cell** command. This command can only be used when the network is not operational.

```
config 802.11 {a | b} pico-cell {enable | disable}
```

Syntax Description	config	Configuration settings.
	802.11	802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	pico-cell	Pico cell extension settings.
	enable disable	Enable or disable this feature.

Defaults None.

Examples To enable pico-cell extensions on an 802.11b network, enter this command:
> config 802.11b pico-cell enable

Related Commands [config 802.11 picocell-V2](#)

config 802.11 picocell-V2

To enable or disable pico cell version 2 mode settings, enter this command:

```
config 802.11{a | b} picocell-V2 {enable | disable}
```

Syntax Description		
config		Configuration settings.
802.11		802.11 network settings.
a b		Specifies 802.11a or 802.11b/g network.
picocell-V2		Picocell version 2.
enable disable		Enable or disable support for this command.

Defaults	None.

Examples	> config 802.11 picocell enable

Related Commands	config 802.11 pico-cell

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		
config		Configuration settings.
802.11		802.11 network settings.
a b		Specifies 802.11a or 802.11b/g network.
rate		Set data rate.
disabled		Disable a specific data rate.
mandatory		Enter mandatory to require a client to support the data rate in order to use the network.
supported		Enter supported to allow any associated client that supports the data rate to use the network.
<i>rate</i>		A rate value of 6, 9, 12, 18, 24, 36, 48, or 54 Mbps.

Defaults None.

Usage Guidelines The data rates set here 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. But it is not required that a client be able to use all the rates marked **supported** in order to associate.

Examples To set 802.11b transmission at a mandatory rate at 12 Mbps, enter this command:

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

Related Commands

show ap config 802.11a
config 802.11b rate

config 802.11 txPower

To configure the transmit power level for all access points or a single access point in an 802.11 network, use the **config 802.11 txPower** command.

```
config 802.11 {a | b} txPower {global [auto | once | power_level]}
config 802.11 {a | b} txPower {ap ap_name [global | power_level]}
```

Syntax Description		
config		Configuration settings.
802.11		802.11 network settings.
a b		Specifies 802.11a or 802.11b/g network.
txPower		Transmit power level settings.
global		The global keyword configures the 802.11 transmit power level for all lightweight access points.
auto once power_level		Optional arguments: auto specifies the power level is automatically set by radio resource management (RRM) for the 802.11 Cisco radio. once specifies the power level is automatically set once by RRM. power_level specifies the transmit power level number.
ap		Configures the 802.11 transmit power level for a specified lightweight access point.
<i>ap_name</i>		The access point name.
global power_level		Optional arguments: global specifies the 802.11 transmit power level is automatically set by RRM and over-rides the existing configuration setting for the access point. power_level specifies a manual transmit power level number for the access point.

Defaults

The command default (**global, auto**) is for automatic configuration by RRM.

Usage Guidelines

The supported power levels depends on the specific access point used and the regulatory region. For example, the 1240 series access point supports eight levels and the 1200 series access point supports six levels. Refer to the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the maximum transmit power limits for your access point. The power levels and available channels are defined by the country code setting and are regulated on a country-by-country basis.

Examples

To have RRM automatically set the 802.11a radio transmit power level in all lightweight access points, enter this command:

```
> config 802.11a txPower global auto
```

To manually set the 802.11b radio transmit power to level 5 for all lightweight access points, enter this command:

```
> config 802.11b txPower global 5
```

To have RRM automatically set the 802.11b radio transmit power for access point AP1, enter this command:

```
> config 802.11b txPower AP1 global
```

To manually set the 802.11a radio transmit power to power level 2 for access point AP1, enter this command:

```
> config 802.11a txPower AP1 2
```

Related Commands

```
show ap config 802.11a
config 802.11b txPower
config country
```

config aaa auth

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

```
config aaa auth mgmt [ aaa_server_type ] [ aaa_server_type ]
```

Syntax Description

mgmt	Configures the AAA authentication search order for controller management users by specifying up to three AAA authentication server types . The order the server types are entered specifies the AAA authentication search order.
<i>aaa_server_type</i>	(Optional) Specifies the AAA authentication server type (local , radius , or tacacs). The local setting specifies the local database, the radius setting specifies the RADIUS server, and the tacacs setting specifies the TACACS+ server.

Defaults

None.

Usage Guidelines

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

Examples

```
> config aaa auth mgmt radius local
```

Related Commands

[show aaa auth](#)

config aaa auth mgmt

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

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

Syntax Description

mgmt	Configure the order of authentication when multiple databases are configured
[radius tacacs]	• (Optional) Enter radius to configure the order of authentication for radius servers. • (Optional) Enter tacacs to configure the order of authentication for tacacs servers.

Defaults

None.

Examples

```
> config aaa auth mgmt radius
> config aaa auth mgmt tacacs
```

Related Commands

show aaa auth order

config acl apply

To apply the Access Control List (ACL) to the data path, use the **config acl apply** command.

config acl apply *rule_name*

**Note**

For a Cisco 2100 series wireless LAN controller, you must configure a pre-authentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any pre-authentication ACL for Cisco 4400 series wireless LAN controllers.

Syntax Description

config acl	Command action.
apply	Applies the ACL (name with up to 32 alphanumeric characters) to the data path.
<i>rule_name</i>	ACL name up to 32 alphanumeric characters.

Defaults

None.

Examples

```
> config acl apply acl01
```

Related Commands

show acl

config acl counter

To see if packets are hitting any of the ACLs configured on your controller, use the **config acl counter** command.

config acl counter {start | stop}



Note ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

Syntax Description

config acl	Command action.
counter {start stop}	Enables or disables ACL counters for your controller.

Defaults

config acl counter stop

Examples

> **config acl counter start**

Related Commands

clear acl counters
show acl detailed

config acl create

To create a new ACL, use the **config acl create** command.

config acl create *rule_name*

**Note**

For a Cisco 2100 series wireless LAN controller, you must configure a pre-authentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any pre-authentication ACL for Cisco 4400 series wireless LAN controllers.

Syntax Description

config acl	Command action.
create	Create a new ACL.
<i>rule_name</i>	ACL name up to 32 alphanumeric characters.

Defaults

None.

Examples

```
> config acl create acl01
```

Related Commands

show acl

config acl cpu

To create a new ACL rule that restricts the traffic reaching the CPU, use the **config acl cpu** command. This allows you to control the type of packets reaching the CPU.

```
config acl cpu rule_name {wired | wireless | both}
```

Syntax Description	config acl cpu	Command action.
	None	Disable the CPU ACL.
	rule_name	ACL name up to 32 alphanumeric characters.
	wired	Enable ACL on wired traffic.
	wireless	Enable ACL on wireless traffic
	both	Enable ACL on both wired and wireless traffic.

Defaults None.

Examples The following example shows how to create an ACL named acl101 on the CPU and apply it to wired traffic.

```
> config acl cpu acl101 wired
```

Related Commands [show acl cpu](#)

config acl delete

To delete an ACL, use the **config acl delete** command.

config acl delete *rule_name*



Note For a Cisco 2100 series wireless LAN controller, you must configure a pre-authentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any pre-authentication ACL for Cisco 4400 series wireless LAN controllers.

Syntax Description

config acl	Command action.
delete	Delete an ACL.
<i>rule_name</i>	ACL name up to 32 alphanumeric characters.

Defaults

None.

Examples

```
> config acl delete acl01
```

Related Commands

show acl

config acl rule

To configure ACL rules, use the **config acl rule** command.

```
config acl rule {
    action rule_name rule_index {permit | deny} |
    add rule_name rule_index |
    change index rule_name old_index new_index |
    delete rule_name rule_index |
    destination address rule_name rule_index ip_address netmask |
    destination port range rule_name rule_index start_port end_port |
    direction rule_name rule_index {in | out | any} |
    dscp rule_name rule_index dscp |
    protocol rule_name rule_index protocol |
    source address rule_name rule_index ip_address netmask |
    source port range rule_name rule_index start_port end_port |
    swap index rule_name index_1 index_2}
```



Note

For a Cisco 2100 series wireless LAN controller, you must configure a pre-authentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any pre-authentication ACL for Cisco 4400 series wireless LAN controllers.

Syntax Description

config acl	Command action.
rule	Configures ACL rules.
action	Configures a rule's action whether to permit or deny access.
add	Adds a new rule.
change	Changes a rule's index.
delete	Deletes a rule.
destination address	Configures a rule's destination IP address and netmask.
destination port range	Configures a rule's destination port range.
direction	Configures a rule's direction to in, out, or any.
dscp	Configures a rule's DSCP.
protocol	Configures a rule's IP Protocol.
source address	Configures a rule's source IP address, netmask.
source port range	Configures a rule's source port range.
swap	Swaps two rules' indices.
<i>rule_name</i>	ACL name up to 32 alphanumeric characters.
<i>rule_index</i>	Rule index between 1 and 32.
<i>ip_address</i>	The rule's IP Address.
<i>netmask</i>	The rule's netmask.
<i>start_port</i>	The start port number (between 0 and 65535).
<i>end_port</i>	The end port number (between 0 and 65535).

<i>dscp</i>	A number between 0 and 63, or any .
<i>protocol</i>	A number between 0 and 255, or any .

Defaults

None.

Examples

```
> config acl rule action lab1 4 permit
```

Related Commands`show acl`

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 7920 VISE parameters, use the **config advanced 802.11 7920VSIEConfig** command.

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

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	7920VSIEConfig	Configure 7920 VISE parameters.
	call-admission-limit G711-CU-Quantum	- Enter call-admission-limit to configure the call admission limit for the 7920s. - Enter G711-CU-Quantum to configure the value supplied by the infrastructure indicating the current number of channel utilization units which would be used by a single G.711-20ms call.
	limit	Call admission limit (from 0 to 255). The default value is 105.
	quantum	G711 quantum value. The default value is 15.

Defaults None.

Examples > config advanced 802.11b 7920VSIEConfig call-admission-limit 4

Related Commands None.

Configure Advanced 802.11 Channel Commands

Use the **config advanced 802.11 channel** commands to configure Dynamic Channel Assignment (DCA) settings on supported 802.11 networks.

config advanced 802.11 channel dca anchor-time

To specify the time of day when the DCA algorithm is to start, use the **config advanced 802.11 channel dca anchor-time** command.

```
config advanced 802.11 { a | b } channel dca anchor-time value
```

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	channel	RRM channel selections.
	dca	Dynamic channel assignment.
	anchor-time	Time when DCA algorithm starts.
	value	Hour of the time between 0 and 23. These values represent the hour from 12:00 a.m. to 11:00 p.m.

Defaults None.

Examples > config advanced 802.11a channel dca anchor-time 17

Related Commands [config advanced 802.11 channel dca interval](#)
[config advanced 802.11 channel dca sensitivity](#)
[show advanced 802.11 channel](#)

config advanced 802.11 channel dca chan-width-11n

To configure the DCA channel width for all 802.11n radios in the 5-GHz band, use this command.

config advanced 802.11{a | b} channel dca chan-width-11n {20 | 40}

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	channel	RRM channel selections.
	dca	Dynamic channel assignment.
	chan-width-11n	Channel width for all 802.11n radios.
	20	Sets the channel width for 802.11n radios to 20 MHz.
	40	Sets the channel width for 802.11n radios to 40 MHz.

Defaults Channel width is 20.

Usage Guidelines If you choose 40, be sure to set at least two adjacent channels in the **config advanced 802.11 channel {add | delete} channel_number** command (for example, a primary channel of 36 and an extension channel of 40). If you set only one channel, that channel is not used for 40-MHz channel width.

To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20- or 40-MHz mode using the **config 802.11 chan_width** command. If you ever then change the static configuration to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

Examples

```
> config advanced 802.11a channel dca chan-width-11n 40
```

Related Commands

- [config 802.11 chan_width](#)
- [config advanced 802.11 channel dca interval](#)
- [config advanced 802.11 channel dca sensitivity](#)
- [show advanced 802.11 channel](#)

config advanced 802.11 channel dca interval

To specify how often the DCA algorithm is allowed to run, use the **config advanced 802.11 channel dca interval** command.

config advanced 802.11 {a | b} **channel dca interval** *value*

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	channel	RRM channel selections.
	dca	Dynamic channel assignment.
	interval	How often the DCA algorithm is allowed to run.
	<i>value</i>	Valid values are 0, 1, 2, 3, 4, 6, 8, 12, or 24 hours. 0 is 10 minutes (600 seconds).

Defaults 0 (10 minutes).

Usage Guidelines If your controller supports only OfficeExtend access points, Cisco recommends that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.

Examples > **config advanced 802.11 channel dca interval 8**

Related Commands [config advanced 802.11 channel dca anchor-time](#)
[config advanced 802.11 channel dca sensitivity](#)
[show advanced 802.11 channel](#)

config advanced 802.11 channel dca sensitivity

To specify how sensitive the DCA algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels, use the **config advanced 802.11 channel dca sensitivity** command.

config advanced 802.11{a | b} channel dca sensitivity {low | medium | high}

Syntax Description

config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
channel	RRM channel selections.
dca	Dynamic channel assignment.
sensitivity	DCA algorithm sensitivity.
low	DCA algorithm is not particularly sensitive to environmental changes. See the “Usage Guidelines” section for more information.
medium	DCA algorithm is moderately sensitive to environmental changes. See the “Usage Guidelines” section for more information.
high	DCA algorithm is highly sensitive to environmental changes. See the “Usage Guidelines” section for more information.

Defaults

None.

Usage Guidelines

The DCA sensitivity thresholds vary by radio band, as noted below:

	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

Examples

```
> config advanced 802.11a channel dca sensitivity low
```

Related Commands

[config advanced 802.11 channel dca anchor-time](#)
[config advanced 802.11 channel dca interval](#)
[show advanced 802.11 channel](#)

config advanced 802.11 channel foreign

To have RRM consider or ignore foreign 802.11a interference avoidance in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel foreign** command.

config advanced 802.11 {a | b} channel foreign {enable | disable}

Syntax	Description
config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
channel	RRM channel selections.
foreign	Foreign interference.
enable disable	Enable foreign access point 802.11a interference avoidance in the channel assignment. Disable foreign access point 802.11a interference avoidance in the channel assignment.

Defaults Enabled.

Examples To have RRM consider foreign 802.11a interference when making channel selection updates for all 802.11a Cisco lightweight access points:

```
> config advanced 802.11a channel foreign enable
```

Related Commands

```
show advanced 802.11a channel
config advanced 802.11b channel foreign
```

config advanced 802.11 channel load

To have RRM consider or ignore traffic load in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel load** command.

```
config advanced 802.11{a | b} channel load {enable | disable}
```

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	channel	RRM channel selections.
	load	Traffic load.
	enable disable	Enable the Cisco lightweight access point 802.11a load avoidance in the channel assignment.
		Disable the Cisco lightweight access point 802.11a load avoidance in the channel assignment.

Defaults Disabled.

Examples To have RRM consider traffic load when making channel selection updates for all 802.11a Cisco lightweight access points:

```
> config advanced 802.11a channel load enable
```

Related Commands

```
show advanced 802.11a channel
config advanced 802.11b channel load
```

config advanced 802.11 channel noise

To have RRM consider or ignore non-802.11a noise in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel noise** command.

config advanced 802.11 {a | b} channel noise {enable | disable}

Syntax Description

config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
channel	RRM channel selections.
noise	Non-802.11a noise.
enable disable	Enable non-802.11a noise avoidance in the channel assignment. or ignore. Disable non-802.11a noise avoidance in the channel assignment.

Defaults

Disabled.

Examples

To have RRM consider non-802.11a noise when making channel selection updates for all 802.11a Cisco lightweight access points:

```
> config advanced 802.11a channel noise enable
```

Related Commands

show advanced 802.11a channel
config advanced 802.11b channel noise

config advanced 802.11 channel update

To have RRM initiate a channel selection update for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel update** command.

config advanced 802.11{a | b} channel update

Syntax Description

config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
channel update	Have RRM update the channel selections.

Defaults

None.

Examples

```
> config advanced 802.11a channel update
```

Related Commands

show advanced 802.11a channel
config advanced 802.11b channel update

Configure Advanced 802.11 Coverage Commands

Use the **config advanced 802.11 coverage** commands to configure coverage hole detection settings on supported 802.11 networks.

config advanced 802.11 coverage

To enable or disable coverage hole detection, use the **config advanced 802.11 coverage** command.

config advanced 802.11{ a | b } **coverage** { enable | disable }

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	coverage	Coverage hole detection.
	enable disable	Enable or disable coverage hole detection.

Defaults Enabled.

Usage Guidelines If you enable coverage hole detection, the controller automatically determines, based on data that is received from the access points, whether any access points have clients that are potentially located in areas with poor coverage.

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples > **config advanced 802.11a coverage enable**

Related Commands

- config advanced 802.11 coverage exception global**
- config advanced 802.11 coverage fail-rate**
- config advanced 802.11 coverage level global**
- config advanced 802.11 coverage packet-count**
- config advanced 802.11 coverage rssi-threshold**
- show advanced 802.11 coverage**

config advanced 802.11 coverage exception global

To specify the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point, use the **config advanced 802.11 coverage exception global** command.

config advanced 802.11{a | b} coverage exception global *percent*

Syntax Description

config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
coverage	Coverage hole detection.
exception	Specifies the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point.
global	Specifies the parameter for all 802.11a access points.
<i>percent</i>	Percentage of clients. Valid values are from 0 to 100%.

Defaults

25%.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11a coverage exception global 50
```

Related Commands

[config advanced 802.11 coverage](#)
[config advanced 802.11 coverage fail-rate](#)
[config advanced 802.11 coverage level global](#)
[config advanced 802.11 coverage packet-count](#)
[config advanced 802.11 coverage rssi-threshold](#)
[show advanced 802.11 coverage](#)

config advanced 802.11 coverage fail-rate

To specify the failure rate threshold for uplink data or voice packets, use the **config advanced 802.11 coverage fail-rate** command.

config advanced 802.11{a | b} **coverage** {data | voice} **fail-rate** *percent*

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	coverage	Coverage hole detection.
	data	Specifies threshold for data packets.
	voice	Specifies threshold for voice packets.
	fail-rate	Configures the threshold count for minimum uplink failures for data or voice packets.
	<i>percent</i>	The failure rate as a percentage. Valid values are from 1 to 100 percent.

Defaults 20.

Usage Guidelines If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples
 > **config advanced 802.11a coverage data fail-rate 80**

Related Commands
config advanced 802.11 coverage
config advanced 802.11 coverage exception global
config advanced 802.11 coverage level global
config advanced 802.11 coverage packet-count
config advanced 802.11 coverage rssi-threshold
show advanced 802.11 coverage

config advanced 802.11 coverage level global

To specify the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold, use the **config advanced 802.11 coverage level global** command.

config advanced 802.11{a | b} coverage level global *clients*

Syntax Description

config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
coverage	Coverage hole detection.
level	Specifies the minimum number of clients on an access point with an RSSI value at or below the RSSI threshold.
global	Specifies the parameter for all 802.11a access points.
<i>clients</i>	Minimum number of clients. Valid values are from 1 to 75.

Defaults

3.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11a coverage level global 60
```

Related Commands

config advanced 802.11 coverage
config advanced 802.11 coverage exception global
config advanced 802.11 coverage fail-rate
config advanced 802.11 coverage packet-count
config advanced 802.11 coverage rssi-threshold
show advanced 802.11 coverage

config advanced 802.11 coverage packet-count

To specify the minimum failure count threshold for uplink data or voice packets, use the **config advanced 802.11 coverage packet-count** command.

config advanced 802.11 {a | b} **coverage** {data | voice} **packet-count** *packets*

Syntax Description

config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
coverage	Coverage hole detection.
data	Specifies threshold for data packets.
voice	Specifies threshold for voice packets.
packet-count	Configures the threshold count for minimum uplink failures for data or voice packets.
<i>packets</i>	Minimum number of packets. Valid values are from 1 to 255 packets.

Defaults

10.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11a coverage data packet-count 100
```

Related Commands

config advanced 802.11 coverage
config advanced 802.11 coverage exception global
config advanced 802.11 coverage fail-rate
config advanced 802.11 coverage level global
config advanced 802.11 coverage rssi-threshold
show advanced 802.11 coverage

config advanced 802.11 coverage rssi-threshold

To specify the minimum receive signal strength indication (RSSI) value for packets that are received by an access point, use the **config advanced 802.11 coverage rssi-threshold** command.

config advanced 802.11{a | b} coverage {data | voice} rssi-threshold *rssi*

Syntax Description

config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
coverage	Coverage hole detection.
data	Specifies threshold for data packets.
voice	Specifies threshold for voice packets.
rssi-threshold	Receive signal strength indication threshold.
<i>rssi</i>	Valid values are from -60 to -90 dBm.

Defaults

- Data packets: -80 dBm.
- Voice packets: -75 dBm.

Usage Guidelines

The *rssi* value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data or voice queue with an RSSI value that is below the value that you enter here, a potential coverage hole has been detected.

The access point takes RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11a coverage data rssi-threshold -60
```

Related Commands

[config advanced 802.11 coverage](#)
[config advanced 802.11 coverage exception global](#)
[config advanced 802.11 coverage fail-rate](#)
[config advanced 802.11 coverage level global](#)
[config advanced 802.11 coverage packet-count](#)
[show advanced 802.11 coverage](#)

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 }

Syntax Description	
config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
edca-parameters	Enables a specific EDCA profile.
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.

Defaults wmm-default

Examples > config advanced 802.11a edca-parameters svp-voice

Related Commands show 802.11a
config advanced 802.11b edca-parameters

config advanced 802.11 factory

To reset 802.11a advanced settings back to the factory defaults, use the **config advanced 802.11 factory** command.

config advanced 802.11{a | b} factory

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	factory	Return all 802.11a advanced settings to their factory defaults.

Defaults	None.

Examples	> config advanced 802.11a factory

Related Commands	show advanced 802.11a channel

config advanced 802.11 group-mode

To set the 802.11a automatic RF group selection mode on or off, use the **config advanced 802.11 group-mode** command.

config advanced 802.11 {a | b} group-mode {auto | off}

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	group-mode	Cisco radio RF grouping.
	auto off	Enter auto to set the 802.11a RF group selection to automatic update mode. Enter off to set the 802.11a RF group selection off.

Defaults Auto.

Examples

To turn the 802.11a automatic RF group selection mode on:

```
> config advanced 802.11a group-mode auto
```

To turn the 802.11a automatic RF group selection mode off:

```
> config advanced 802.11a group-mode off
```

Related Commands

```
show advanced 802.11a group
config advanced 802.11b group-mode
```

Configure Advanced 802.11 Logging Commands

Use the **config advanced 802.11 logging** commands to configure report log settings on supported 802.11 networks.

config advanced 802.11 logging channel

To turn the channel change logging mode on or off, use the **config advanced 802.11 logging channel** command.

config advanced 802.11{a | b} logging channel {on | off}

Syntax Description

config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
logging channel	Log channel changes.
on off	Enable or disable 802.11a channel logging.

Defaults

Off (disabled).

Examples

```
> config advanced 802.11 logging channel on
```

Related Commands

show advanced 802.11a logging
config advanced 802.11b logging channel

config advanced 802.11 logging coverage

To turn the coverage profile logging mode on or off, use the **config advanced 802.11 logging coverage** command.

config advanced 802.11 {a | b} logging coverage {on | off}

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	logging coverage	Log coverage changes.
	on off	Enable or disable 802.11a coverage profile violation logging.

Defaults Off (disabled).

Examples > **config advanced 802.11a logging coverage on**

Related Commands **show advanced 802.11a logging**
config advanced 802.11b logging coverage

config advanced 802.11 logging foreign

To turn the foreign interference profile logging mode on or off, use the **config advanced 802.11 logging foreign** command.

```
config advanced 802.11{a | b} logging foreign {on | off}
```

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	logging foreign	Log foreign changes.
	on off	Enable or disable 802.11a foreign interference profile violation logging.

Defaults Off (disabled).

Examples > config advanced 802.11a logging foreign on

Related Commands show advanced 802.11a logging
config advanced 802.11b logging foreign

config advanced 802.11 logging load

To turn the 802.11a load profile logging mode on or off, use the **config advanced 802.11 logging load** command.

config advanced 802.11{a | b} logging load {on | off}

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	logging load	Log load changes.
	on off	Enable or disable 802.11a load profile violation logging.

Defaults	Off (disabled).

Examples	> config advanced 802.11a logging load on

Related Commands	show advanced 802.11a logging config advanced 802.11b logging load

config advanced 802.11 logging noise

To turn the 802.11a noise profile logging mode on or off, use the **config advanced 802.11 logging noise** command.

```
config advanced 802.11{a | b} logging noise {on | off}
```

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	logging noise	Log noise changes.
	on off	Enable or disable 802.11a noise profile violation logging.

Defaults Off (disabled).

Examples > config advanced 802.11a logging noise on

Related Commands show advanced 802.11a logging
config advanced 802.11b logging noise

config advanced 802.11 logging performance

To turn the 802.11a performance profile logging mode on or off, use the **config advanced 802.11 logging performance** command.

config advanced 802.11 {a | b} logging performance {on | off}

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	logging performance	Log performance changes.
	on off	Enable or disable 802.11a performance profile violation logging.

Defaults	Off (disabled).

Examples	> config advanced 802.11 logging performance on

Related Commands	show advanced 802.11a logging config advanced 802.11b logging performance

config advanced 802.11 logging txpower

To turn the 802.11a transmit power change logging mode on or off, use the **config advanced 802.11 logging txpower** command.

```
config advanced 802.11{a | b} logging txpower {on | off}
```

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	logging txpower	Log power changes.
	on off	Enable or disable 802.11a transmit power change logging.

Defaults Off (disabled).

Examples > config advanced 802.11 logging txpower off

Related Commands show advanced 802.11 logging
config advanced 802.11b logging power

Configure Advanced 802.11 Monitor Commands

Use the **config advanced 802.11 monitor** commands to configure monitor settings on supported 802.11 networks.

config advanced 802.11 monitor channel-list

To set the 802.11a noise, interference, and rogue monitoring channel list, use the **config advanced 802.11 monitor channel-list** command.

```
config advanced 802.11 {a | b} monitor channel-list {all | country | dca}
```

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	monitor channel-list	Monitor coverage interval.
	all country dca	- Enter all to monitor all channels. - Enter country to monitor the channels used in the configured country code. - Enter dca to monitor the channels used by the automatic channel assignment.

Defaults	country.

Examples	> config advanced 802.11a monitor channel-list country

Related Commands	show advanced 802.11a monitor coverage

config advanced 802.11 monitor coverage

To set the coverage measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor coverage** command.

```
config advanced 802.11{a | b} monitor coverage seconds
```

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	monitor coverage	Monitor coverage interval.
	seconds	Coverage measurement interval between 60 and 3600 seconds.

Defaults 180 seconds.

Examples To set the coverage measurement interval to 60 seconds:
> config advanced 802.11 monitor coverage 60

Related Commands show advanced 802.11a monitor
config advanced 802.11b monitor coverage

config advanced 802.11 monitor load

To set the load measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor load** command.

config advanced 802.11{a | b} **monitor load** *seconds*

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	monitor load	Monitor load interval.
	<i>seconds</i>	Load measurement interval between 60 and 3600 seconds.

Defaults 60 seconds.

Examples To set the load measurement interval to 60 seconds:
> **config advanced 802.11a monitor load 60**

Related Commands **show advanced 802.11a monitor**
config advanced 802.11b monitor load

config advanced 802.11 monitor mode

To enable or disable 802.11a access point monitoring, use the **config advanced 802.11 monitor mode** command.

```
config advanced 802.11{a | b} monitor mode {enable | disable}
```

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	monitor mode	Monitor mode.
	enable disable	Enable or disable 802.11a access point monitoring.

Defaults	Enabled.

Examples	> config advanced 802.11a monitor mode enable

Related Commands	show advanced 802.11a monitor config advanced 802.11b monitor mode

config advanced 802.11 monitor noise

To set the 802.11a noise measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor noise** command.

config advanced 802.11{a | b} **monitor noise** *seconds*

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	monitor noise	Monitor noise interval.
	<i>seconds</i>	Noise measurement interval between 60 and 3600 seconds.

Defaults	180 seconds.

Examples	To set the noise measurement interval to 120 seconds: > config advanced 802.11a monitor noise 120

Related Commands	show advanced 802.11a monitor config advanced 802.11b monitor noise

config advanced 802.11 monitor signal

To set the signal measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor signal** command.

config advanced 802.11{a | b} monitor signal *seconds*

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	monitor signal	Monitor signal interval.
	<i>seconds</i>	Signal measurement interval between 60 and 3600 seconds.

Defaults	60 seconds.

Examples	To set the signal measurement interval to 120 seconds: > config advanced 802.11a monitor signal 120

Related Commands	show advanced 802.11a monitor config advanced 802.11b monitor signal

Configure Advanced 802.11 Profile Commands

Use the **config advanced 802.11 profile** commands to configure Cisco lightweight access point profile settings on supported 802.11 networks.

config advanced 802.11 profile clients

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

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

Syntax Description	
config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
profile clients	Cisco lightweight access point Client profile
{ global <i>cisco_ap</i> }	- Enter global to configure all 802.11a Cisco lightweight access points. - Enter a Cisco lightweight access point name.
<i>clients</i>	802.11a Cisco lightweight access point client threshold between 1 and 75 clients.

Defaults 12 clients.

Examples To set all Cisco lightweight access point clients thresholds to 25 clients:

```
> config advanced 802.11a profile clients global 25
```

Global client count profile set.

To set the AP1 clients threshold to 75 clients:

```
> config advanced 802.11a profile clients AP1 75
```

Global client count profile set.

Related Commands

show advanced 802.11a profile
config advanced 802.11b profile clients

config advanced 802.11 profile customize

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

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

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	customize	Performance profile.
	cisco_ap	Cisco lightweight access point.
	on off	Enter on to customize performance profiles for this Cisco lightweight access point. Enter off to use global default performance profiles for this Cisco lightweight access point.

Defaults Off.

Examples To turn performance profile customization on for 802.11a Cisco lightweight access point AP1:
> config advanced 802.11 profile customize AP1 on

Related Commands show advanced 802.11 profile
config advanced 802.11b profile customize

config advanced 802.11 profile foreign

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

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

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	profile foreign	Foreign interference profile.
	{global cisco_ap}	Global or Cisco lightweight access point specific profile.
	percent	802.11a foreign 802.11a interference threshold between 0 and 100 percent.

Defaults 10.

Examples

To set the Other 802.11a transmitter interference threshold for all Cisco lightweight access points to 50 percent:

```
> config advanced 802.11a profile foreign global 50
```

To set the Other 802.11a transmitter interference threshold for AP1 to 0 percent:

```
> config advanced 802.11a profile foreign AP1 0
```

Related Commands

show advanced 802.11a profile

config advanced 802.11b profile foreign

config advanced 802.11 profile noise

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

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

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	profile noise	Profile noise limits.
	global cisco_ap	Global or Cisco lightweight access point specific profile.
	dBm	802.11a foreign noise threshold between -127 and 0 dBm.

Defaults -70 dBm.

Examples

To set the 802.11a foreign noise threshold for all Cisco lightweight access points to -127 dBm:

```
> config advanced 802.11 profile noise global -127
```

To set the 802.11a foreign noise threshold for AP1 to 0 dBm:

```
> config advanced 802.11 profile noise AP1 0
```

Related Commands

show advanced 802.11 profile

config advanced 802.11b profile noise

config advanced 802.11 profile throughput

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

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

Syntax Description		
	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	profile throughput	Data rate threshold.
	global cisco_ap	Global or Cisco lightweight access point specific profile.
	<i>value</i>	802.11a Cisco lightweight access point throughput threshold between 1000 and 10000000 bytes per second.

Defaults 1,000,000 bytes per second.

Examples To set all Cisco lightweight access point data-rate thresholds to 1000 bytes per second:

```
> config advanced 802.11 profile data-rate global 1000
```

To set the AP1 data-rate threshold to 10000000 bytes per second:

```
> config advanced 802.11 profile data-rate AP1 10000000
```

Related Commands

show advanced 802.11 profile

config advanced 802.11b profile data-rate

config advanced 802.11 profile utilization

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

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

Syntax Description

config	Configuration settings.
advanced 802.11	Advanced 802.11 network settings.
a b	Specifies 802.11a or 802.11b/g network.
profile utilization	Cisco lightweight access point profile utilization
global cisco_ap	Global or Cisco lightweight access point specific profile.
percent	802.11a RF utilization threshold between 0 and 100 percent.

Defaults

80 percent.

Examples

To set the RF utilization threshold for all Cisco lightweight access points to 0 percent:

```
> config advanced 802.11a profile utilization global 0
```

To set the RF utilization threshold for AP1 to 100 percent:

```
> config advanced 802.11a profile utilization AP1 100
```

Related Commands

show advanced 802.11a profile

config advanced 802.11b profile utilization

config advanced 802.11 receiver

To set the advanced receiver configuration settings, use the **config advanced 802.11 receiver** command.

```
config advanced 802.11 {a | b} receiver default
config advanced 802.11 {a | b} receiver rxstart jumpThreshold value
config advanced 802.11 {a | b} receiver pico-cell-V2 send_iapp_req client_mac
```

Syntax Description		
config		Configuration settings.
advanced 802.11		Advanced 802.11 network settings.
a b		Specifies 802.11a or 802.11b/g network.
receiver		Receiver configuration.
default		Default advanced receiver configuration.
rxstart jumpThreshold		Receiver start signal.
<i>value</i>		Jump threshold configuration value between 0 and 127.
pico-cell-V2		Pico cell version 2 parameters.
send_iapp_req		Send a unicast IAPP high-density frame request.
<i>client_mac</i>		The client MAC address.

Defaults None.

Examples To prevent changes to receiver parameters while network is enabled:
 > **config advanced802.11a receiver default**

Related Commands **config advanced 802.11b receiver**

config advanced 802.11 txpower-update

To initiate updates of the 802.11a transmit power for every Cisco lightweight access point, use the **config advanced 802.11 txpower-update** command.

config advanced 802.11{a | b} txpower-update

Syntax Description	config	Configuration settings.
	advanced 802.11	Advanced 802.11 network settings.
	a b	Specifies 802.11a or 802.11b/g network.
	txpower-update	Update transmission power.

Defaults	None.

Examples	> config advanced 802.11a txpower-update

Related Commands	config advance 802.11b txpower-update

config advanced backup-controller primary

To configure a primary backup controller for a specific controller, use the **config advanced backup-controller primary** command.

```
config advanced backup-controller primary backup_controller_name
                                         backup_controller_ip_address
```

Syntax Description	config	Configuration settings.
	advanced	Advanced parameters.
	backup-controller primary	Configure the primary backup controller.
	<i>backup_controller_name</i>	Name of the backup controller.
	<i>backup_controller_ip_address</i>	IP address of the backup controller.

Defaults	None.

Usage Guidelines	To delete a primary backup controller entry, enter 0.0.0.0 for the controller IP address.

Examples	> config advanced backup-controller primary Controller_1 10.10.10.10

Related Commands	show advanced backup-controller

config advanced backup-controller secondary

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

```
config advanced backup-controller secondary backup_controller_name  
                                backup_controller_ip_address
```

Syntax Description	config	Configuration settings.
	advanced	Advanced parameters.
	backup-controller secondary	Configure the secondary backup controller.
	<i>backup_controller_name</i>	Name of the backup controller.
	<i>backup_controller_ip_address</i>	IP address of the backup controller.

Defaults	None.

Usage Guidelines	To delete a secondary backup controller entry, enter 0.0.0.0 for the controller IP address.

Examples	> config advanced backup-controller secondary Controller_1 10.10.10.10

Related Commands	show advanced backup-controller

config advanced client-handoff

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

config advanced client-handoff *num_of_retries*

Syntax Description

config	Configuration settings.
advanced	Advanced parameters.
client-handoff	Client handoff.
<i>num_of_retries</i>	Number of excessive retries before client handoff (from 0 to 255).

Defaults

0 excessive retries (disabled).

Examples

To set the client handoff to 100 excessive retries:

```
> config advanced client-handoff 100
```

Related Commands

show advanced client-handoff

config advanced dot11-padding

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

config advanced dot11-padding {enable | disable}

Syntax Description

config	Configuration settings.
advanced	Advanced settings.
dot11-padding	Over-the-air frame padding settings.
enable disable	Enable or disable this command.

Defaults

Disabled.

Examples

To enable over-the-air frame padding, enter this command:

```
> config advanced dot11-padding enable
```

Related Commands

```
debug dot11
debug dot11 mgmt interface
debug dot11 mgmt msg
debug dot11 mgmt ssid
debug dot11 mgmt state-machine
debug dot11 mgmt station
show advanced dot11-padding
```

config advanced assoc-limit

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

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

Syntax Description	[enable disable]	Enable or disable the feature.
	<i>number of associations per interval</i>	The number of association request per access point slot in a given interval. The valid range is 1 to 100.
	<i>interval in milliseconds</i>	The association request limit interval. The valid range is 100 to 10000.

Defaults Disabled.

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

Examples > **config advanced assoc-limit enable 20 250**

config advanced eap

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

```
config advanced eap [ eapol-key-timeout timeout | eapol-key-retries retries |
  identity-request-timeout timeout |
  identity-request-retries retries |
  key-index index |
  max-login-ignore-identity-response {enable | disable}
  request-timeout timeout |
  request-retries retries ]
```

Syntax Description		
eapol-key-timeout	(Optional) Specifies the amount of time (1 to 5 seconds) in which the controller attempts to send an EAP key over the LAN to wireless clients using local EAP.	
eapol-key-retries	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller attempts to send an EAP key over the LAN to wireless clients using local EAP.	
identity-request-timeout	(Optional) Specifies the amount of time (1 to 120 seconds) in which the controller attempts to send an EAP identity request to wireless clients using local EAP.	
identity-request-retries	(Optional) Specifies the maximum number of times (1 to 20 retries) that the controller attempts to retransmit the EAP identity request to wireless clients using local EAP.	
key-index	(Optional) index—Specifies the key index (0 or 3) used for dynamic wired equivalent privacy (WEP).	
max-login-ignore-identity-response	(Optional) Specifies that the maximum EAP identity response login count for a user is ignored. When enabled, this command limits the number of devices that can be connected to the controller with the same username.	
request-timeout	(Optional) Specifies the amount of time (1 to 120 seconds) in which the controller attempts to send an EAP request to wireless clients using local EAP..	
request-retries	(Optional) Specifies the maximum number of times (1 to 120 retries) that the controller attempts to retransmit the EAP request to wireless clients using local EAP.	

Defaults

Default for **eapol-key-timeout**: 1 second.

Default for **eapol-key-retries**: 2 retries.

Examples

```
> config advanced eap key-index 0
```

Related Commands

show advanced eap

config advanced rate

To enable or disable switch control path rate limiting, use the **config advanced rate** command.

config advanced rate [enable | disable]

Syntax Description	config	Configuration parameters
	advanced	Advanced configuration parameters.
	rate	Configure control path rate limiting parameters.
	enable disable	Enable or disable the feature.

Defaults	None.

Examples	To enable switch control path rate limiting, enter the following command: > config advanced rate enable

Related Commands	None.

config advanced statistics

To enable or disable the Cisco Wireless LAN controller port statistics collection, use the **config advanced statistics** command.

```
config advanced statistics {enable | disable}
```

Syntax Description	config	Configuration settings.
	advanced	Advanced parameters.
	statistics	Statistics.
	{enable disable}	Enable or disable switch port statistics.

Defaults Enabled.

Examples To disable statistics:
> config advanced statistics disable

Related Commands show advanced statistics
show stats port
show stats switch

config advanced probe filter

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

config advanced probe filter {enable | disable}

Syntax Description	config	Configuration parameters.
	advanced	Advanced configuration parameters.
	probe	Configure probe parameters.
	filter	Configure probe filtering.
	enable disable	Enable or disable this feature.

Defaults	None.

Examples	To enable the filtering of probe requests forwarded from an access point to the controller, enter the following command: <pre>> config advanced probe filter enable</pre>

Related Commands	config advanced probe limit config radius acct fallback-test show advanced probe show radius acct statistics

config advanced probe limit

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

config advanced probe limit *num_probes interval*

Syntax Description

config	Configuration parameters.
advanced	Advanced configuration parameters.
probe	Configure probe parameters.
limit	Configure probe number and interval.
<i>num_probes</i>	Number of probe requests (from 1 to 100) forwarded to the controller per client per access point radio in a given interval.
<i>interval</i>	Probe limit interval (from 100 to 10000 milliseconds).

Defaults

Default *num_probes* is 2 probe requests.
Default *interval* is 500 milliseconds.

Examples

To set the number of probes per access point per client to 5 and the probe interval to 800 milliseconds, enter the following command:

```
> config advanced probe limit 5 800
```

Related Commands

[config advanced probe filter](#)
[config radius acct fallback-test](#)
[show advanced probe](#)

Configure Advanced Timers Commands

User the **advanced timers** commands to configure advanced 802.11a settings.

config advanced timers ap-discovery-timeout

The Cisco lightweight access point discovery time-out is how often a Cisco Wireless LAN controller attempts to discover unconnected Cisco lightweight access points. 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	config	Configuration settings.
	advanced	Advanced parameters.
	timers	Network timers.
	ap-discovery-timeout	Cisco lightweight access point discovery timeout.
	<i>seconds</i>	Timeout value between 1 and 10 seconds.

Defaults 10 seconds.

Examples > **config advanced timers ap-discovery-timeout 20**

Related Commands

- [show advanced timers](#)
- [config advanced timers ap-fast-heartbeat](#)
- [config advanced timers ap-heartbeat-timeout](#)
- [config advanced timers ap-primary-discovery-timeout](#)
- [config advanced timers auth-timeout](#)

config advanced timers ap-fast-heartbeat

To enable or disable the fast heartbeat timer thus reducing the amount of time it takes to detect a controller failure for local, hybrid-REAP, or all access points, use the **config advanced timers ap-fast-heartbeat** command.

config advanced timers ap-fast-heartbeat {local | hreap | all} {enable | disable} *interval*

Syntax Description	config	Configuration settings.
	advanced	Advanced parameters.
	timers	Network timers.
	ap-fast-heartbeat	Configure the fast heartbeat interval
	{local hreap all}	- Enable local to configure the fast heartbeat interval for access points in local mode only. - Enable hreap to configure the fast heartbeat interval for access points in hybrid-REAP mode only. - Enable all to configure the fast heartbeat interval for all access points.
	{enable disable}	- Select enable to enable a fast heartbeat interval. - Select disable to disable a fast heartbeat interval
	<i>interval</i>	Specify a small heartbeat interval (between 1 and 10 seconds inclusive) reduces the amount of time it takes to detect a controller failure.

Defaults Disabled.

Examples

```
> config advanced timers ap-fast-heartbeat local enable 5
> config advanced timers ap-fast-heartbeat hreap enable 8
> config advanced timers ap-fast-heartbeat all enable 6
> config advanced timers ap-fast-heartbeat all disable
```

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 auth-timeout](#)

config advanced timers ap-heartbeat-timeout

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. 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	config	Configuration settings.
	advanced	Advanced parameters.
	timers	Network timers.
	ap-heartbeat-timeout	Cisco lightweight access point heartbeat timeout.
	<i>seconds</i>	Timeout value between 1 and 30 seconds.

Defaults 30 seconds.

Usage Guidelines This *seconds* value should be at least three times larger than the fast heartbeat timer.

Examples

```
> 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	config	Configuration settings.
	advanced	Advanced parameters.
	timers	Network timers.
	ap-primary-discovery-timeout	Configure the amount of time the access point will wait for a discovery response from a controller.
	interval	Timeout value between 30 and 3600 seconds.

Defaults 120 seconds.

Examples > 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	config	Configuration settings.
	advanced	Advanced parameters.
	timers	Network timers.
	auth-timeout	Authentication response timeout.
	<i>seconds</i>	Timeout value in seconds between 10 and 600.

Defaults	10 seconds.

Examples	> config advanced timers auth-timeout 20

Related Commands	show advanced timers config advanced timers ap-fast-heartbeat config advanced timers ap-discovery-timeout config advanced timers ap-heartbeat-timeout config advanced timers ap-primary-discovery-timeout

config advanced timers eap-timeout

To configure the EAP expiration timeout, use the **config advanced timers eap-timeout** command.

config advanced timers eap-timeout *seconds*

Syntax Description	config	Configuration settings.
	advanced	Advanced parameters.
	timers	Network timers.
	eap-timeout	EAP timeout.
	<i>seconds</i>	Timeout value in seconds between 8 and 120.

Defaults	None.

Examples	> config advanced timers eap-timeout 10

Related Commands	show advanced timers

config advanced timers eap-identity-request-delay

To configure the advanced EAP identity request delay in seconds, use the **config advanced timers eap-identity-request-delay** command.

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

Syntax Description	show	Display settings.
	advanced	Advanced parameters.
	timers	Advanced system timers.
	eap-identity-request-delay	
	<i>seconds</i>	Number of seconds between 0 and 10.

Defaults None.

Examples > `show advanced timers eap-identity-request-delay 8`

Related Commands config advanced timers auth-timeout, config advanced timers rogue-ap, show advanced timers

Configure Access Point Commands

User the **config ap** commands to configure access point settings.

config ap

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

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

Syntax Description

config	Configuration settings.
ap	Access point settings.
enable disable	Enable or disable this command.
cisco_ap	Name of the Cisco lightweight access point.
add delete	Add or delete a foreign access point.
MAC	MAC address of a foreign access point.
port	Port number through which the foreign access point can be reached.
IP_address	IP address of the foreign access point.

Defaults

None.

Examples

To disable lightweight access point AP1, enter this command:

```
> config ap disable AP1
```

To add a foreign access point with MAC address 12:12:12:12:12:12 and IP address 192.12.12.1 from port 2033, enter this command:

```
> config ap add 12:12:12:12:12:12 2033 enable 192.12.12.1
```

Related Commands

[Configure Access Point Commands](#)
[Show Access Point Commands](#)

config ap bhmode

To configure the Cisco Bridge Backhaul Mode, use the **config ap bhmode** command.

config ap bhmode {11a | 11b | 11g} cisco_ap

Syntax Description		
config		Display settings.
ap		Advanced parameters.
bhmode		Configure the Cisco Bridge Backhaul Mode.
11a 11b 11g		- Enter 11a to set 11a as the Cisco Bridge Backhaul Mode. - Enter 11b to set 11b as the Cisco Bridge Backhaul Mode. - Enter 11g to set 11g as the Cisco Bridge Backhaul Mode.
<i>cisco_ap</i>		Name of a Cisco lightweight access point.

Defaults None.

Examples

```
> config ap bhmode 11g AP02
```

Changing the AP's backhaul mode will cause the AP to reboot.
Are you sure you want to continue? (y/n)

Related Commands **config ap**

config ap bhrate

To configure the Cisco Bridge Backhaul Tx Rate, use the **config ap bhrate** command.

```
config ap bhrate {rate | auto} cisco_ap
```

Syntax Description	config	Display settings.
	ap	Advanced parameters.
	bhrate	Configure Cisco Bridge Backhaul Tx Rate.
	rate	Cisco Bridge Backhaul Tx Rate in Kbps. The valid values are: 6000, 12000, 18000, 24000, 36000, 48000, and 54000.
	auto	Configures auto data rate.
	cisco_ap	Name of a Cisco lightweight access point.

Defaults Auto.

Usage Guidelines

In previous software releases, the default value for bridge data rate was **24000** (24 Mbps). In controller software release 6.0, the default value for bridge data rate is **auto**. If you configured the default bridge data rate value (24000) in a previous controller software release, the bridge data rate is configured with the new default value (auto) when you upgrade to controller software release 6.0. However, if you configured a non-default value (for example, 18000) in a previous controller software release, that configuration setting is preserved when you upgrade to software release 6.0.

When the bridge data rate is set to **auto**, the mesh backhaul chooses the highest rate where the next higher rate cannot be used due to unsuitable conditions for that specific rate (and not because of conditions that affect all rates).

Examples

```
> config ap bhrate 54000 AP01
```

Related Commands

config ap

config ap bridgegroupname

To set or delete a bridge group name on a Cisco lightweight access point, use the **config ap bridgegroupname** command.

config ap bridgegroupname {set *groupname* | delete} *cisco_ap*

Syntax Description	config	Display settings.
	ap	Access point settings.
	bridgegroupname	Set or delete bridgegroupname on a Cisco lightweight access point.
	set <i>groupname</i> delete	- Enter set <i>groupname</i> to set a Cisco lightweight access point's bridge group name. - Enter delete to delete a Cisco lightweight access point's bridge group name.
	<i>cisco_ap</i>	Name of a Cisco lightweight access point.

Defaults None.

Usage Guidelines Only access points with the same bridge group name can connect to each other.

Examples

```
> config ap bridgegroupname delete AP02
```

Changing the AP's bridgegroupname may strand the bridge AP. Please continue with caution.
Changing the AP's bridgegroupname will also cause the AP to reboot.
Are you sure you want to continue? (y/n)

Related Commands **config ap**

config ap bridging

To enable or disable Ethernet-to-Ethernet bridging on a Cisco lightweight access point, use the **config ap bridging** command.

```
config ap bridging {enable | disable} cisco_ap
```

Syntax Description	config	Display settings.
	ap	Advanced parameters.
	bridging	enable or disable Ethernet-to-Ethernet bridging on a Cisco lightweight access point.
	{enable disable}	Enable or disable Ethernet-to-Ethernet bridging.
	cisco_ap	Name of a Cisco lightweight access point.

Defaults None.

Examples

To enable bridging on an access point enter:

```
config ap bridging enable nyc04-44-1240
```

To disable bridging on an access point enter:

```
config ap bridging disable nyc04-44-1240
```

Related Commands config ap

config ap cdp

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

```
config ap cdp {enable | disable} {cisco_ap | all}
```

Syntax Description

config	Configuration settings.
ap	Configure lightweight access points.
cdp	Cisco Discovery Protocol.
enable disable	Enable or disable CDP.
cisco_ap all	Name of a Cisco lightweight access point or all to specify all access points.

Defaults

Disabled.

Usage Guidelines

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



Note

After you enable CDP on all access points joined to the controller, you may disable and then re-enable CDP on individual access points using **config ap cdp {enable | disable} cisco_ap**. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.

Examples

```
> config ap cdp enable all
> config ap cdp disable ap02
```

Related Commands

[config cdp timer](#)
[show ap cdp](#)

config ap core-dump

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

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

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point settings.
	core-dump	Configure a Cisco lightweight access point’s memory core dump.
	enable disable	Enable or disable this feature.
	tftp_server_ipaddress	IP address of the TFTP server to which the access point sends core dump files.
	filename	The name the access point uses to label the core file.
	compress uncompress	- Enter compress to compress the core dump file. - Enter uncompress to not compress the core dump file.
	cisco_ap all	Name of a Cisco lightweight access point or all to specify all access points.

Defaults None.

Usage Guidelines The access point must be able to reach the TFTP server.

Examples > config ap core-dump enable 192.1.1.1 log compress AP02

Related Commands [config ap crash-file clear-all](#)
[config ap crash-file delete](#)
[config ap crash-file get-crash-file](#)
[config ap crash-file get-radio-core-dump](#)
[config ap port](#)

config ap crash-file clear-all

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

config ap crash-file clear-all

Syntax Description	config	Display settings.
	ap	Advanced parameters.
	crash-file clear-all	Delete all crash and radio core dump files.

Defaults	None.

Examples	> config ap crash-file clear-all

Related Commands	config ap core-dump config ap crash-file delete config ap crash-file get-crash-file config ap crash-file get-radio-core-dump config ap port

config ap crash-file delete

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

config ap crash-file delete *filename*

Syntax Description

config	Display settings.
ap	Advanced parameters.
crash-file delete	Delete a single crash or radio core dump file.
<i>filename</i>	Name of the file to delete.

Defaults

None.

Examples

```
> config ap crash-file delete crash-file-1
```

Related Commands

[config ap core-dump](#)
[config ap crash-file clear-all](#)
[config ap crash-file get-crash-file](#)
[config ap crash-file get-radio-core-dump](#)
[config ap port](#)

config ap crash-file get-crash-file

To collect the latest crash data for a Cisco lightweight access point, use the **config ap crash-file get-crash-file** command. Use the [transfer upload datatype](#) command to transfer the collected data to the Cisco Wireless LAN controller.

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

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	crash-file	Collect the latest crash data for an access point.
	get-crash-file	
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults None.

Examples
 > **config ap crash-file get-crash-file AP3**

Related Commands

- [config ap core-dump](#)
- [config ap crash-file clear-all](#)
- [config ap crash-file delete](#)
- [config ap crash-file get-radio-core-dump](#)
- [config ap port](#)

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

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

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

Syntax Description	config	Display settings.
	ap	Advanced parameters.
	crash-file radio-core-dump	Get a Cisco lightweight access point’s radio core dump.
	Slot_ID	The slot ID (either 0 or 1).
	cisco_ap	Name of a Cisco lightweight access point.

Defaults None.

Examples > config ap crash-file get-radio-core-dump 0 AP02

Related Commands

- config ap core-dump
- config ap crash-file clear-all
- config ap crash-file delete
- config ap crash-file get-crash-file
- config ap port

config ap dot1xuser

To configure the global authentication username and password for all access points currently joined to the controller as well as any access points that join the controller in the future, enter this command. Alternatively, you can set the values for a specific access point.

```
config ap dot1xuser add username user password password {all | cisco_ap}
```

Syntax Description		
config		Configuration settings.
ap		Cisco lightweight access point.
dot1xuser		Descriptive location.
add username		Add username.
<i>user</i>		Specify username.
password		Add password.
<i>password</i>		Specify password.
all		For all access points.
<i>cisco_ap</i>		For a specific access point.

Defaults None.

Usage Guidelines You must enter a strong *password*. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of upper- and lowercase letters, numbers, and symbols.
- They are not a word in any language.

Examples

```
config ap dot1xuser add username cisco123 password cisco2020 all
config ap dot1xuser add username cisco123 password cisco2020 cisco_ap
```

Related Commands

- [config ap dot1xuser delete](#)
- [config ap dot1xuser disable](#)
- [show ap summary](#)

config ap dot1xuser delete

To force a specific access point to use the controller’s global authentication settings, enter the following command:

```
config ap dot1xuser delete cisco_ap
```

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	dot1xuser	Descriptive location.
	delete	Delete authentication.
	cisco_ap	Specify the access point.

Defaults None.

Examples config ap mgmtuser delete cisco_ap1

Related Commands

- config ap dot1xuser
- config ap dot1xuser disable
- show ap summary

config ap dot1xuser disable

To disable authentication for all access points or for a specific access point, enter the following command:

```
config ap dot1xuser disable {all | cisco_ap}
```

Syntax Description

config	Configuration settings.
ap	Cisco lightweight access point.
dot1xuser	Descriptive location.
disable	Delete authentication.
all	For all access points.
<i>cisco_ap</i>	Specify the access point

Defaults

None.

Usage Guidelines

You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

Examples

```
config ap mgmtuser disable cisco_ap1
```

Related Commands

[config ap dot1xuser](#)
[config ap dot1xuser delete](#)
[show ap summary](#)

config ap group-name

To specify a descriptive group name for a Cisco lightweight access point, use the **config ap group-name** command. The Cisco lightweight access point must be disabled before changing this parameter.

```
config ap group-name groupname cisco_ap
```

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point settings.
	groupname	Descriptive name for the access point group.
	cisco_ap	Name of the Cisco lightweight access point.

Defaults None.

Examples > config ap group-name superusers AP01

Related Commands

- config ap group-name
- config wlan apgroup
- show ap summary
- show ap wlan

config ap h-reap radius auth set

To configure a primary or secondary RADIUS server for a specific hybrid-REAP access point, use the **config ap h-reap radius auth set** command.

```
config ap h-reap radius auth set {primary | secondary}ip_address auth_port secret
```

Syntax Description	config ap	Configure access point.
	h-reap	Enter h-reap to specify the hybrid remote edge access point mode.
	radius auth set	
	primary	
	secondary	
	ip_address	Name of the Cisco lightweight access point.
	auth_port secret	

Defaults
None.

Examples
> config ap h-reap radius auth set primary 192.12.12.1

Related Commands

- config ap mode h-reap
- config ap h-reap vlan wlan
- config ap h-reap vlan
- config ap h-reap vlan native

config ap h-reap vlan

To enable or disable VLAN tagging for a hybrid-REAP access, use the **config ap h-reap vlan** command.

```
config ap h-reap vlan {enable | disable} cisco_ap
```

Syntax Description	config ap	Configure access point.
	h-reap	Enter h-reap to specify the hybrid remote edge access point mode.
	{enable disable}	Enable or disable the access point's VLAN tagging.
	cisco_ap	Name of the Cisco lightweight access point.

Defaults Disabled. Once enabled, WLANs enabled for local switching inherit the VLAN assigned at the controller.

Examples > config ap h-reap vlan wlan enable AP02

- Related Commands**
- config ap mode h-reap
 - config ap h-reap radius auth set
 - config ap h-reap vlan wlan
 - config ap h-reap vlan native

config ap h-reap vlan native

To configure a native VLAN for a hybrid-REAP access, use the **config ap h-reap vlan native** command.

config ap h-reap vlan native *vlan-id* *cisco_ap*

Syntax Description	config ap	Configure access point.
	h-reap	Enter h-reap to specify the hybrid remote edge access point mode.
	vlan native	The “managing” VLAN.
	<i>vlan-id</i>	VLAN identifier.
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults	None.

Examples	> config ap h-reap vlan native 6 AP02

Related Commands	config ap mode h-reap config ap h-reap radius auth set config ap h-reap vlan wlan

config ap h-reap vlan wlan

To assign a VLAN ID to a hybrid-REAP access point, use the **config ap h-reap vlan wlan** command.

```
config ap h-reap vlan wlan ip_address vlan-id cisco_ap
```

Syntax Description	config ap	Configure access point.
	h-reap	Enter h-reap to specify the hybrid remote edge access point mode.
	ip_address	Name of the Cisco lightweight access point.
	vlan-id	VLAN identifier.
	cisco_ap	Name of the Cisco lightweight access point.

Defaults VLAN ID associated to the WLAN.

Examples > config ap h-reap vlan wlan 192.12.12.1 6 AP02

- Related Commands
- config ap mode h-reap
 - config ap h-reap radius auth set
 - config ap h-reap vlan
 - config ap h-reap vlan native

config ap led-state

To enable or disable the LED-State for an access point, use the **config ap led-state** command.

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

Syntax Description	config	Display settings.
	ap	Advanced parameters.
	led-state	Enable or disable the LED-State for an access point.
	{enable disable}	Enable or disable the access point's LED-State.
	{cisco_ap all}	Name of a Cisco lightweight access point or all to specify all access points.

Defaults	None.

Examples	> config ap led-state enable AP02

Related Commands	config ap

config ap link-encryption

To enable Datagram Transport Layer Security (DTLS) data encryption for access points on the 5500 series controller, use the **config ap link-encryption** command.

config ap link-encryption {enable | disable} {Cisco_AP | all}

Syntax Description

config	Display settings.
ap	Advanced parameters.
link-encryption	Enable or disable data encryption for an access point.
{enable disable}	Enable or disable the access point's LED-State.
{Cisco_AP all}	Name of a Cisco lightweight access point or all to specify all access points.

Defaults

DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points.

Usage Guidelines

Only 5500 series controllers support DTLS data encryption. This feature is not available on other controller platforms. If an access point with data encryption enabled tries to join any other controller, the access point joins the controller, but data packets are sent unencrypted.

Only 1130, 1140, 1240, and 1250 series access points support DTLS data encryption, and data-encrypted access points can join a 5500 series controller only if the wplus license is installed on the controller. If the wplus license is not installed, the access points cannot join the controller.

Examples

```
> config ap link-encryption enable AP02
```

Related Commands

config ap
[show dtls connections](#)

config ap link-latency

To enable or disable link latency for a specific access point or for all access points currently associated to the controller, enter this command:

```
config ap link-latency {enable | disable | reset} {cisco_ap | all}
```

Syntax Description

config	Configuration settings.
ap	Cisco lightweight access point.
link-latency	Configure link-latency.
enable disable	Enable or disable link-latency.
reset	Reset all link-latency statistics.
<i>cisco_ap</i>	Name of the Cisco lightweight access point.
all	Configure all Cisco access points.

Defaults

Link latency is disabled by default.

Usage Guidelines

This command enables or disables link latency only for access points that are currently joined to the controller. It does not apply to access points that join in the future.

Examples

```
>config ap link-latency enable all
```

Related Commands

[show ap config](#)

config ap location

To modify the descriptive location of a Cisco lightweight access point, use the **config ap location** command. The Cisco lightweight access point must be disabled before changing this parameter.

```
config ap location location cisco_ap
```

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	location	Descriptive location.
	location	Location name (enclosed by double quotation marks).
	cisco_ap	Name of the Cisco lightweight access point.

Defaults None.

Examples > config ap location "Building 1" AP1

Related Commands show ap summary

config ap location

To modify the descriptive location of a Cisco lightweight access point, use the **config ap location** command. The Cisco lightweight access point must be disabled before changing this parameter.

config ap location *location cisco_ap*

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	location	Descriptive location.
	<i>location</i>	Location name (enclosed by double quotation marks).
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults	None.

Examples	> config ap location "Building 1" AP1

Related Commands	show ap summary

config ap logging

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

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

Syntax Description

config	Configuration settings.
logging	Syslog facility logging.
syslog	System logs.
level	Syslog message severity level
<i>severity_level</i>	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
<i>cisco_ap</i>	Cisco access point.
all	All access points.

Defaults

None.

Usage Guidelines

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

Examples

```
> config ap logging syslog level 3
```

Related Commands

config logging syslog host
config logging syslog facility
show logging

config ap mgmtuser delete

To force a specific access point to use the controller's global credentials, enter the following command:

```
config ap mgmtuser delete cisco_ap
```

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	mgmtuser	Descriptive location.
	delete	Delete local credentials.
	<i>cisco_ap</i>	Specify the access point

Defaults	None.

Examples	<pre>>config ap mgmtuser delete cisco_ap1</pre>

Related Commands	<pre>show ap summary</pre>

config ap mode

To change a Cisco wireless LAN controller communication option for an individual Cisco lightweight access point, use the **config ap mode** command.

```
config ap mode { bridge | h-reap | local | reap | rogue | sniffer |  
                  monitor [submode { none | wips } ] } cisco_ap
```

Syntax Description

config	Configuration settings.
ap	Access point settings.
mode	Controller communication options.
bridge	Convert from a lightweight access point to a mesh access point (bridge mode).
h-reap	Enable hybrid remote edge access point mode on an access point.
local	Convert from an indoor mesh access point (MAP or RAP) to a non-mesh lightweight access point (local mode).
reap	Enable remote edge access point mode on an access point.
rogue	Enable rogue detector mode on an access point.
sniffer	Enable wireless sniffer mode on an access point.
monitor	Configure Cisco wireless intrusion prevention system (wIPS) monitor mode on an access point.
submode	Configure wIPS submode on an access point.
none wips	- Enter none to disable wIPS on an access point. - Enter wips to enable wIPS submode on an access point.
<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults

Local.

Usage Guidelines

Sniffer mode will capture and forward all the packets from the clients on that channel to a remote machine that runs AiroPeek or other supported packet analyzer software. It will include information on timestamp, signal strength, packet size and so on.

Examples

Sets the controller to communicate with access point AP91 in bridge mode:

```
> config ap mode bridge AP91
```

Sets the controller to communicate with access point AP01 in local mode:

```
> config ap mode local AP01
```

Sets the controller to communicate with access point AP91 in remote office (REAP) mode:

```
> config ap mode reap AP91
```

Sets the controller to communicate with access point AP91 in remote office (REAP) mode:

```
> config ap mode h-reap AP01
```

Sets the controller to communicate with access point AP01 in rogue access point detector mode:

```
> config ap mode rogue AP01
```

Sets the controller to communicate with access point AP02 in wireless sniffer mode:

```
> config ap mode sniffer AP02
```

Sets the controller to communicate with access point AP02 in wIPS submode:

```
> config ap mode monitor submode wips AP02
```

Related Commands

[config 802.11 enable](#)
[config ap mode](#)
[config ap monitor-mode](#)
[show ap config](#)
[show ap monitor-mode summary](#)
[show wps wips statistics](#)

config ap monitor-mode

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

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

Syntax Description

config	Configuration settings.
ap	Access point settings.
mode	Controller communication options.
monitor-mode	Monitor mode settings.
802.11b fast-channel	Configure 802.11b scanning channels for a monitor-mode access point.
no-optimization	No channel scanning optimization for the access point.
tracking-opt	Enables tracking optimized channel scanning for the access point.
wips-optimized	Enable wIPS optimized channel scanning for the access point.
<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults

None.

Examples

```
> config ap monitor-mode wips-optimized AP01
```

Related Commands

[config 802.11 enable](#)
[config ap mode](#)
[show ap config](#)
[show ap monitor-mode summary](#)
[show wps wips statistics](#)
[show wps wips summary](#)

config ap name

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

config ap name *new_name old_name*

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	name	Name of the Cisco lightweight access point.
	<i>new_name</i>	Desired Cisco lightweight access point name.
	<i>old_name</i>	Current Cisco lightweight access point name.

Defaults	None.

Examples	> config ap name AP1 AP2

Related Commands	show ap config

config ap port

To configure the port for a Foreign Access Point., use the **config ap port** command.

config ap port *MAC port*

Syntax Description	config	Display settings.
	ap	Advanced parameters.
	port	Configure the port for a Foreign Access Point
	<i>MAC</i>	Foreign Access Point MAC address.
	<i>port</i>	Port number for accessing the Foreign Access Point.

Defaults	None.

Examples	> config ap port 12:12:12:12:12:12 20

Related Commands	config ap

config ap power injector

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

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

Syntax Description		
config		Display settings.
ap		Advanced parameters.
power		Configure the power injector state for an access point.
{ enable disable }		Enable or disable the power injector state for an access point.
<i>cisco_ap</i>		Name of the Cisco lightweight access point.
all		Configure all Cisco lightweight access points connected to the controller.
installed		Detect the MAC address of the current switch port that has a power injector.
override		Override the safety checks and assume a power injector is always installed.
<i>switch_MAC</i>		The MAC address of the switch port with an installed power injector.

Defaults None.

Examples > **config ap power injector enable all 12:12:12:12:12:12**

Related Commands **config ap**

config ap power pre-standard

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

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

Syntax Description	config	Display settings.
	ap	Advanced parameters.
	power pre-standard	Configure the Inline Power Cisco Pre-Standard switch state for an access point.
	{enable disable}	Enable or disable the Inline Power Cisco pre-standard switch state for an access point.
	cisco_ap	Name of the Cisco lightweight access point.

Defaults	Disabled.

Examples	> config ap power pre-standard enable AP02

Related Commands	config ap

config ap primary-base

To set the Cisco lightweight access point primary Cisco Wireless LAN controller, use the **config ap primary-base** command. The Cisco lightweight access point associates with this Cisco Wireless LAN controller for all network operation and in the event of a hardware reset.

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

Syntax Description		
config		Configuration settings.
ap		Cisco lightweight access point.
primary-base		Cisco lightweight access point primary Cisco Wireless LAN controller.
<i>controller_name</i>		Name of Cisco Wireless LAN controller.
<i>cisco_ap</i>		Cisco lightweight access point name.
<i>controller_ip_address</i>		[Optional] If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller.
	Note	For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Defaults None.

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

Examples

```
> config ap primary-base SW_1 AP2
```

Related Commands

- show sysinfo
- config sysname
- config ap secondary-base
- config ap tertiary-base

config ap priority

To assign a priority designation to an access point that allows it to reauthenticate after a controller failure by priority rather than on a first-come-until-full basis, use the **config ap priority** command.

In a failover situation, if the backup controller does not have enough ports to allow all the access points in the affected area to reauthenticate, it gives priority to higher-priority access points over lower-priority ones, even if it means replacing lower-priority access points.

```
config ap priority {1 | 2 | 3 | 4} cisco_ap
```

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	priority	Configure AP failover priority command
	{1 2 3 4}	Assign a reauthentication priority: • 1 to specify low priority • 2 to specify medium priority • 3 to specify high priority • 4 to specify highest (critical) priority
	cisco_ap	Cisco lightweight access point name.

Defaults 1 - Low priority.

Examples > config ap priority 3 AP02

Related Commands [config network ap-priority](#)
[show ap summary](#)
[show network summary](#)

config ap reporting-period

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

config ap reporting-period *period*

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	reporting-period	Reporting-period command.
	<i>period</i>	Time period in seconds between 10 and 120.

Defaults	None.

Examples	> config ap reporting-period 120

Related Commands	show ap config 802.11a
	show ap config 802.11ab

config ap reset

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

```
config ap reset cisco_ap
```

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	reset	Reset command.
	cisco_ap	Cisco lightweight access point name.

Defaults	None.

Examples	> config ap reset AP2

Related Commands	show ap config

config ap role

To specify the role of an access point in a mesh network, use the **config ap role** command.

config ap role {**rootAP** | **meshAP**} *AP_name*

Syntax Description	config	Display settings.
	ap	Access point settings.
	role	Specify the role of an access point in a mesh network.
	rootAP meshAP	- Enter rootAP to designate the mesh access point a root access point (RAP). - Enter meshAP to designate the mesh access point a mesh access point (MAP).
	<i>AP_name</i>	Name of the Cisco lightweight access point.

Defaults **meshAP.**

Usage Guidelines Use the **meshAP** argument if the access point has a wireless connection to the controller, or use the **rootAP** argument if the access point has a wired connection to the controller.

Examples

```
> config ap role rootAP AP02
```

Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)

Related Commands **config ap**

config ap rst-button

To configure the Reset button for an access point, use the **config ap rst-button** command.

```
config ap rst-button {enable | disable} cisco_ap
```

Syntax Description	config	Display settings.
	ap	Advanced parameters.
	rst-button	Configure the Reset button for an access point.
	{enable disable}	Enable or disable the Reset button for an access point.
	cisco_ap	Name of the Cisco lightweight access point.

Defaults None.

Examples > config ap rst-button enable AP03

Related Commands config ap

config ap secondary-base

To set the Cisco lightweight access point secondary Cisco Wireless LAN controller, use the **config ap secondary-base** command. The Cisco lightweight access point associates with this Cisco Wireless LAN controller for all network operation and in the event of a hardware reset.

config ap secondary-base *controller_name* *cisco_ap* [*controller_ip_address*]

Syntax Description		
config		Configuration settings.
ap		Cisco lightweight access point.
primary-base		Cisco lightweight access point secondary Cisco Wireless LAN controller.
<i>controller_name</i>		Name of Cisco Wireless LAN controller.
<i>cisco_ap</i>		Cisco lightweight access point name.
<i>controller_ip_address</i>		[Optional] If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller.
	Note	For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Defaults None.

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

Examples

```
> config ap secondary-base SW_1 AP2
```

Related Commands

- show sysinfo
- config sysname
- config ap primary-base
- config ap tertiary-base

config ap sniff

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

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

Syntax Description

config	Configuration settings.
ap	Configure access point.
sniff	Sniffer command.
802.11a 802.11b	Specifies type of 802.11 network.
enable disable	Enable or disable sniffing.
<i>channel</i>	Channel to be sniffed.
<i>server_ip</i>	The IP address of the remote machine running Omnippeek, Airopeek, AirMagnet, or Wireshark software.
<i>cisco_ap</i>	Access point configured as the sniffer.

Defaults

Channel 36.

Usage Guidelines

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

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

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

Examples

```
> config ap sniff 80211a enable 23 11.22.44.55 AP01
```

Related Commands

[show ap config](#)

config ap sniff 802.11b

config ap ssh

To enable Secure Shell (SSH) connectivity on an access point, use the **config ap ssh** command. The Cisco lightweight access point associates with this Cisco Wireless LAN controller for all network operation and in the event of a hardware reset.

config ap ssh {enable | disable} *cisco_ap*

Syntax Description	config	Configuration settings.
	ap	Configure access point.
	ssh	Configure SSH connectivity on the access point.
	enable disable	Enable or disable this command.
	<i>cisco_ap</i>	Cisco access point name.

Defaults None.

Examples

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

Related Commands

- [config ap](#)
- [config network ssh](#)
- [show ap stats](#)

config ap static-ip

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

```
config ap static-ip {enable cisco_ap ip_address net_mask gateway | disable cisco_ap | add
  {domain {cisco_ap | all} domain_name} | {nameserver {cisco_ap | all} dns_ip_address} |
  delete {domain | nameserver} {cisco_ap | all}}
```

Syntax Description

config	Configuration settings.
ap	Cisco lightweight access point.
static-ip	Configure Cisco lightweight access point static IP address settings.
{enable disable}	Configure the Cisco lightweight access point static IP address. Disable the Cisco lightweight access point static IP address. The access point uses DHCP to get the IP address.
<i>cisco_ap</i>	Cisco lightweight access point name.
<i>ip_address</i>	Cisco lightweight access point IP address
<i>net_mask</i>	The Cisco lightweight access point network mask.
<i>gateway</i>	IP address of the Cisco lightweight access point gateway.
{add delete}	Add or delete a domain or DNS server.
domain	Specify the domain to which a specific access point or all access points belong.
all	All access points.
<i>domain_name</i>	Domain name.
nameserver	Specify a DNS server so that a specific access point or all access points can discover the controller using DNS resolution.
<i>dns_ip_address</i>	DNS server IP address.

Defaults

None.

Usage Guidelines

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

After you enter the IP, netmask, and gateway addresses , save your configuration to reboot the access point. After the access point rejoins the controller, you can enter the domain and DNS server information.

```
> config ap static-ip enable AP2 1.1.1.1 255.255.255.0 10.1.1.1
> save config
>
> config ap static-ip add domain AP2 example_domain
```

Related Commands

show sysinfo

config sysname
config ap secondary-base
config ap primary-base

config ap stats-timer

Use this command to set the time in seconds that the Cisco lightweight access point sends its DOT11 statistics to the Cisco Wireless LAN controller. A value of 0 (zero) means the Cisco lightweight access point will not send any DOT11 statistics. The acceptable range for the timer is from 0 to 65535 seconds, and the Cisco lightweight access point must be disabled to set this value.

```
config ap stats-timer period cisco_ap
```

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	stats-timer	Cisco lightweight access point primary Cisco Wireless LAN controller.
	period	Time in seconds from 0 to 65535. A zero value disables the timer.
	cisco_ap	Cisco lightweight access point name.

Defaults 0 (disabled).

Examples > config ap stats-timer 600 AP2

Related Commands config ap disable

config ap syslog host global

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

config ap syslog host global *syslog_server_IP_address*

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	syslog	System logs.
	host	Remote host.
	global	All Cisco lightweight access points.
	<i>syslog_server_IP_address</i>	IP address of the syslog server.

Defaults 255.255.255.255.

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

Examples > **config ap syslog host global 255.255.255.255**

Related Commands

- config ap syslog host specific**
- show ap config global**
- show ap config general**

config ap syslog host specific

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

```
config ap syslog host specific cisco_ap syslog_server_IP_address
```



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

Syntax Description

config	Configuration settings.
ap	Cisco lightweight access point.
syslog	System logs.
host	Remote host.
specific	A single, specified Cisco access point.
syslog_server_IP_address	IP address of the syslog server.

Defaults

0.0.0.0

Examples

```
> config ap syslog host specific 0.0.0.0
```

Related Commands

- config ap syslog host global
- show ap config global
- show ap config general

config ap tcp-adjust-mss

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

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

Syntax Description

config	Configuration settings.
ap	Configure access point.
tcp-adjust-mss	Configure TCP MSS on the access point.
enable disable	Enable or disable this command.
<i>Cisco_AP</i>	Cisco access point name.
all	All access points.
<i>size</i>	Maximum segment size, from 536 to 1363 bytes.

Defaults

None.

Usage Guidelines

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

Examples

```
> config ap tcp-adjust-mss enable cisco_ap1 1200
```

Related Commands

[show ap tcp-mss-adjust](#)

config ap telnet

To enable Telnet connectivity on an access point, use the **config ap telnet** command. The Cisco lightweight access point associates with this Cisco Wireless LAN controller for all network operation and in the event of a hardware reset.

```
config ap telnet {enable | disable} cisco_ap
```

Syntax Description	config	Configuration settings.
	ap	Configure access point.
	telnet	Configure Telnet connectivity on the access point.
	enable disable	Enable or disable this command.
	cisco_ap	Cisco access point name.

Defaults None.

Examples > config ap telnet enable cisco_ap1
> config ap telnet disable cisco_ap1

Related Commands [config ap](#)
[config network telnet](#)
[show ap config](#)

config ap tertiary-base

To set the Cisco lightweight access point tertiary Cisco Wireless LAN controller, use the **config ap tertiary-base** command. The Cisco lightweight access point associates with this Cisco Wireless LAN controller for all network operation and in the event of a hardware reset.

config ap tertiary-base *controller_name* *cisco_ap* [*controller_ip_address*]

Syntax Description		
config		Configuration settings.
ap		Cisco lightweight access point.
tertiary-base		Cisco lightweight access point tertiary Cisco Wireless LAN controller.
<i>controller_name</i>		Name of Cisco Wireless LAN controller.
<i>cisco_ap</i>		Cisco lightweight access point name.
<i>controller_ip_address</i>		[Optional] If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller.
	Note	For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Defaults None.

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

Examples

```
> config ap tertiary-base SW_1 AP2
```

Related Commands

- show sysinfo
- config sysname
- config ap secondary-base
- config ap primary-base

config ap tftp-downgrade

This command is used to configure the settings used for downgrading a lightweight access point to an autonomous access point.

config ap tftp-downgrade (*tftp_ip_address*) (*image_filename*) (*ap_name*)

Syntax Description	<i>tftp_ip_address</i>	Specifies the IP address of the TFTP server.
	<i>image_filename</i>	Specifies the filename of the access point image file on the TFTP server.
	<i>ap_name</i>	Specifies the access point name.

Defaults	None.

Examples	> config ap tftp-downgrade 10.0.23.8 1238.tar ap1240_102301

Related Commands	show running-config show version

config ap username

To assign a username and password to access either a specific access point or all access points, use this command:

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

Syntax Description

username	Configures the access point's administrator username.
<i>user_id</i>	Specifies the administrator username.
password	Configures the access point's administrator password.
<i>passwd</i>	Specifies the administrator password.
all	Configures all
<i>ap_name</i>	Specifies the name of a specific access point.

Defaults

None.

Examples

To assign a username and password to a specific access point enter a command similar to the following:

```
config ap username jack password blue 1a204
```

To assign the same username and password to all access points enter a command similar to the following:

```
config ap username jack password blue all
```

Related Commands

None.

config ap wlan

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

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

Syntax Description	config	Configuration settings.
	ap	Cisco lightweight access point.
	wlan	Reset command.
	enable disable	Enable or disable per access point wireless LAN override on an access point.
	802.11a 802.11b	Select 802.11a or 802.11b/g radio.
	wlan_id	Optional Cisco Wireless LAN controller ID assigned to a wireless LAN.
	cisco_ap	Cisco lightweight access point name.

Defaults None.

Examples To enable wireless LAN override on the AP03 802.11a radio:
> config ap wlan enable 802.11a AP03

Related Commands [show ap wlan](#)

config auth-list add

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

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

Syntax Description	config auth-list	Command action.
	add	Create an authorized access point entry.
	mic	Access point has manufacture installed certificate.
	ssc	Access point has self-signed certificate.
	<i>AP_MAC</i>	MAC address of a Cisco lightweight access point.
	<i>AP_key</i>	A key hash value equal to 20 bytes or 40 digits.

Defaults	None.

Examples	<pre>> config auth-list add mic 00:0b:85:02:0d:20</pre>

Related Commands	<pre>config auth-list delete</pre> <pre>config auth-list ap-policy</pre>

config auth-list ap-policy

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

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

Syntax Description	config auth-list	Command action.
	ap-policy	Create an authorized access point entry.
	authorize-ap {enable disable}	Enable or disable access point authorization.
	ssc {enable disable}	Enable or disable access point with self-signed certificate to connect.

Defaults	None.

Examples	> config auth-list ap-policy authorize-ap enable
	> config auth-list ap-policy ssc disable

Related Commands	config auth-list add
	config auth-list delete

config auth-list delete

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

config auth-list delete *AP_MAC*

Syntax Description	config auth-list	Command action.
	delete	Delete an access point entry.
	<i>AP_MAC</i>	MAC address of a Cisco lightweight access point.

Defaults	None.

Examples	> config auth-list delete 00:0b:85:02:0d:20

Related Commands	config auth-list add config auth-list ap-policy

config boot

Each Cisco Wireless LAN controller can boot off the primary, last-loaded OS image or boot off the backup, earlier-loaded OS image. To change a Cisco Wireless LAN controller boot option, use the **config boot** command.

```
config boot {primary | backup}
```

Syntax Description	config boot	Configure boot option.
	{primary backup}	Set the primary image or backup image as active.

Defaults	primary

Examples	> config boot primary
	> config boot backup

Related Commands	show boot

config cdp timer

This command is used to configure the CDP maximum hold timer.

config cdp timer *seconds*

Syntax Description	<i>seconds</i> Specifies the maximum hold timer value (5 to 254 seconds).
Defaults	None.
Examples	> config cdp timer 150
Related Commands	None.

config certificate

To configure SSL certificates, use the **config certificate** command.

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

Syntax Description

config	Configuration settings.
certificate	Secure Socket Layer certificate settings.
generate	Authentication certificate generation settings.
webadmin webauth	- Enter webadmin to generate a new web administration certificate. - Enter webauth to generate a new web authentication certificate.
compatibility	Compatibility mode for inter-Cisco Wireless LAN controller IPSEC settings.
on off	Enable or disable Compatibility mode.

Defaults

None.

Examples

```
> config certificate generate webadmin
```

```
Creating a certificate may take some time. Do you wish to continue? (y/n)
```

```
> 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	
config	Configuration settings.
certificate	Secure Socket Layer certificate settings.
lsc	Locally Significant Certificate settings.
enable disable	Enable or disable LSC certificates on the controller.
ca-server	Certificate Authority (CA) server settings.
<i>http://url:port/path</i>	Either a domain name or IP address of the CA server.
ca-cert	CA certificate database settings.
add delete	- Enter add to obtain a CA certificate from the CA server and add it to the controller's certificate database. - Enter delete to delete a CA certificate from the controller's certificate database.
subject-params	Device certificate settings.
<i>country state city orgn dept email</i>	The 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>Cxxx-MacAddr</i> , where <i>xxx</i> is the product number.
other-params	Device certificate keysize settings.
<i>keysize</i>	A value from 384 to 2048 (in bits); the default value is 2048.
ap-provision	Access point provision list settings.
auth-list	Provision list authorization settings.
<i>ap_mac</i>	MAC address of access point to be added or deleted from the provision list.
revert-cert	The number of times the access point attempts to join the controller using an LSC before reverting to the default certificate.
<i>retries</i>	A 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 will 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 non-zero value.

Defaults

Default value of *keysize* is 2048 bits.
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 using the **config certificate lsc ca-server delete** command, 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 MIC or SSC certificate that join the controller are LSC provisioned.

Examples

```
config certificate lsc enable
config certificate lsc ca-server http://10.0.0.1:8080/caserver
config certificate lsc ca-cert add
config certificate lsc subject-params US CA Anytown Acme_Inc. IT_dept joegeek@acme.com
config certificate lsc keysize 2048
config certificate lsc ap-provision auth-list add xx:xx:xx:xx:xx:xx
config certificate lsc ap-provision revert-cert 6
```

Related Commands

[config certificate](#)
[show certificate compatibility](#)
[show certificate lsc](#)
[show certificate summary](#)
[show local-auth certificates](#)

Configure Client Commands

User the **config client** commands to configure client settings.

config client ccx clear-reports

To clear the client reporting information, use the **config client ccx clear-reports** command.

config client ccx clear-reports *client_mac_address*

Syntax Description	<i>client_mac_address</i> Specifies the MAC address of the client.

Defaults	None.

Examples	> config client ccx clear-reports 172.19.28.40

Related Commands	config client ccx get-profiles config client ccx get-operating-parameters config client ccx get-manufacturer-info config client ccx get-client-capability show client ccx profiles show client ccx operating-parameters show client ccx manufacturer-info show client ccx client-capability config client ccx stats-request show client ccx stats-report

config client ccx clear-results

To clear the test results on the controller, use the **config client ccx clear-results** command.

config client ccx clear-results *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

None.

Examples

> **config client deauthenticate 172.19.28.40**

Related Commands

config client ccx default-gw-ping
config client ccx
config client ccx dns-ping
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

config client ccx default-gw-ping

To send a request to the client to perform the default gateway ping test, use the **config client ccx default-gw-ping** command.

config client ccx default-gw-ping *client_mac_address*



Note This test does not require the client to use the diagnostic channel.

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

None.

Examples

```
> config client ccx default-gw-ping 00:E0:77:31:A3:55
```

Related Commands

config client ccx dhcp-test
config client ccx dns-ping
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

config client ccx dhcp-test

To send a request to the client to perform the DHCP test, use the **config client ccx dhcp-test** command.

config client ccx dhcp-test *client_mac_address*



Note This test does not require the client to use the diagnostic channel.

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

None.

Examples

```
> config client ccx dhcp-test 00:E0:77:31:A3:55
```

Related Commands

config client ccx default-gw-ping
config client ccx dns-ping
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

config client ccx dns-ping

To send a request to the client to perform the DNS server IP address ping test, use the **config client ccx dns-ping** command.

config client ccx dns-ping *client_mac_address*



Note This test does not require the client to use the diagnostic channel.

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

None.

Examples

```
> config client ccx dns-ping 00:E0:77:31:A3:55
```

Related Commands

config client ccx default-gw-ping
config client ccx dhcp
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

config client ccx dns-resolve

To send a request to the client to perform the DNS name resolution test to the specified host name, use the **config client ccx dns-resolve** command.

config client ccx dns-resolve *client_mac_address* *host_name*



Note This test does not require the client to use the diagnostic channel.

Syntax Description

<i>client_mac_address</i>	Specifies the MAC address of the client.
<i>host_name</i>	Specifies the host name of the client.

Defaults

None.

Examples

```
> config client ccx dns resolve 00:E0:77:31:A3:55 host_name
```

Related Commands

config client ccx default-gw-ping
config client ccx dhcp
config client ccx dns-ping
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

config client ccx get-client-capability

To send a request to the client to send its capability information, use the **config client ccx get-client-capability** command.

config client ccx get-client-capability *client_mac_address*

Syntax Description	<i>client_mac_address</i> Specifies the MAC address of the client.

Defaults	None.

Examples	<pre>> config client ccx get-client-capability 172.19.28.40</pre>

Related Commands	- config client ccx get-profiles - config client ccx get-operating-parameters - config client ccx get-manufacturer-info - config client ccx clear-reports - show client ccx profiles - show client ccx operating-parameters - show client ccx manufacturer-info - show client ccx client-capability - config client ccx stats-request - show client ccx stats-report

config client ccx get-manufacturer-info

To send a request to the client to send the manufacturer's information, use the **config client ccx get-manufacturer-info** command.

config client ccx get-manufacturer-info *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

None.

Examples

> config client ccx get-manufacturer-info 172.19.28.40

Related Commands

config client ccx get-profiles
config client ccx get-operating-parameters
config client ccx get-client-capability
config client ccx clear-reports
show client ccx profiles
show client ccx operating-parameters
show client ccx manufacturer-info
show client ccx client-capability
config client ccx stats-request
show client ccx stats-report

config client ccx get-operating-parameters

To send a request to the client to send its current operating parameters, use the **config client ccx get-operating-parameters** command.

config client ccx get-operating-parameters *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

None.

Examples

> **config client ccx get-operating-parameters 172.19.28.40**

Related Commands

config client ccx get-profiles
config client ccx get-manufacturer-info
config client ccx get-client-capability
config client ccx clear-reports
show client ccx profiles
show client ccx operating-parameters
show client ccx manufacturer-info
show client ccx client-capability
config client ccx stats-request
show client ccx stats-report

config client ccx get-profiles

To send a request to the client to send its profiles, use the **config client ccx get-profiles** command.

config client ccx get-profiles *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

None.

Examples

> **config client ccx get-profiles 172.19.28.40**

Related Commands

config client ccx get-operating-parameters
config client ccx get-manufacturer-info
config client ccx get-client-capability
config client ccx clear-reports
show client ccx profiles
show client ccx operating-parameters
show client ccx manufacturer-info
show client ccx client-capability
config client ccx stats-request
show client ccx stats-report

config client ccx log-request

To configure a Cisco client extension (CCX) log request for a specified client device, use the **config client CCX log-request** command.

config client ccx log-request *log_type* [**roam** | **rsna** | **syslog**] *client_mac_address*

Syntax Description

roam	Specifies the request to specify the client CCX roaming log.
rsna	Specifies the request to specify the client CCX RSNA log.
syslog	Specifies the request to specify the client CCX system log.
<i>client_mac_address</i>	Specifies the MAC address of the client.

Defaults

None.

Examples

```
> config client ccx log-request syslog 00:40:96:a8:f7:98
> show client ccx log-response syslog 00:40:96:a8:f7:98

Tue Oct 05 13:05:21 2006
  SysLog Response LogID=1: Status=Successful
  Event Timestamp=121212121212
  Client SysLog = 'This is a test syslog 2'
  Event Timestamp=121212121212
  Client SysLog = 'This is a test syslog 1'
Tue Oct 05 13:04:04 2006
  SysLog Request LogID=1

> config client ccx log-request roam 00:40:96:a8:f7:98
> show client ccx log-response roam 00:40:96:a8:f7:98

Thu Jun 22 11:55:14 2006
  Roaming Response LogID=20: Status=Successful
  Event Timestamp=121212121212
  Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
  Transition Time=100(ms)
  Transition Reason: Unspecified Transition Result: Success
Thu Jun 22 11:55:04 2006
  Roaming Request LogID=20
Thu Jun 22 11:54:54 2006
  Roaming Response LogID=19: Status=Successful
  Event Timestamp=121212121212
  Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
  Transition Time=100(ms)
  Transition Reason: Unspecified Transition Result: Success
Thu Jun 22 11:54:33 2006  Roaming Request LogID=19

> config client ccx log-request rsna 00:40:96:a8:f7:98
> show client ccx log-response rsna 00:40:96:a8:f7:98

Tue Oct 05 11:06:48 2006
  RSNA Response LogID=2: Status=Successful
  Event Timestamp=242424242424
  Target BSSID=00:0b:85:23:26:70
  RSNA Version=1
  Group Cipher Suite=00-0f-ac-01
```

```

Pairwise Cipher Suite Count = 2
    Pairwise Cipher Suite 0 = 00-0f-ac-02
    Pairwise Cipher Suite 1 = 00-0f-ac-04
AKM Suite Count = 2
    KM Suite 0 = 00-0f-ac-01
    KM Suite 1 = 00-0f-ac-02
SN Capability = 0x1
PMKID Count = 2
    PMKID 0 = 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
    PMKID 1 = 0a 0b 0c 0d 0e 0f 17 18 19 20 1a 1b 1c 1d 1e 1f
802.11i Auth Type: EAP_FAST
RSNA Result: Success
Tue Oct 05 11:05:48 2006
RSNA Request LogID=2

```

Related Commands show client ccx log-response

config client ccx send-message

To send a message to the client, use the **config client ccx send-message** command.

config client ccx send-message *client_mac_address message_id*

Syntax Description	
<i>client_mac_address</i>	Specifies the MAC address of the client.
<i>message_type</i>	Involves one of the following: 1—The SSID is invalid. 2—The network settings are invalide 3—There is a WLAN credibility mismatch. 4—The user credentials are incorrect. 5—Please call support. 6—The problem is resolved. 7—The problem has not been resolved. 8—Please try again later. 9—Please correct the indicated problem. 10—Troubleshooting is refused by the network. 11—Retrieving client reports. 12—Retrieving client logs. 13—Retrieval complete. 14—Beginning association test. 15—Beginning DHCP test. 16—Beginning network connectivitiy test. 17—Beginning DNS ping test. 18—Beginning name resolution test. 19—Beginning 802.1X authentication test. 20—Redirecting client to a specific profile. 21—Test complete. 22—Test passed. 23—Test failed. 24—Cancel diagnostic channel operation or select a WLAN profile to resume normal operation. 25—Log retrieval refused by the client. 26—Client report retrieval refused by the client. 27—Test request refused by the client. 28—Invalid network (IP) setting. 29—There is a known outage or problem with the network. 30—Scheduled maintenance period. (continued on next page)

-
<i>message_type</i> (cont.)	• 31—The WLAN security method is not correct. • 32—The WLAN encryption method is not correct. • 33—The WLAN authentication method is not correct.
-

Defaults

None.

Examples

```
> config client ccx send-message 172.19.28.40 user-action-required
```

Related Commands

```

config client ccx default-gw-ping
config client ccx dhcp
config client ccx dns-ping
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

```

config client ccx stats-request

To send a request for statistics, use the **config client ccx stats-request** command.

config client ccx stats-request *measurement_duration stats_name* [**dot11** | **security**]
client_mac_address

Syntax Description

<i>duration</i>	Specifies the measurement duration in seconds.
dot11	Specifies dot11 counters.
security	Specifies security counters.
<i>client_mac_address</i>	Specifies the MAC address of the client.

Defaults

None.

Examples

```
> config client ccx stat-request 1 dot11 00:40:96:a8:f7:98
> show client ccx stat-report 00:40:96:a8:f7:98
```

Measurement duration = 1

```
dot11TransmittedFragmentCount      = 1
dot11MulticastTransmittedFrameCount = 2
dot11FailedCount                   = 3
dot11RetryCount                    = 4
dot11MultipleRetryCount            = 5
dot11FrameDuplicateCount           = 6
dot11RTSSuccessCount               = 7
dot11RTSFailureCount              = 8
dot11ACKFailureCount              = 9
dot11ReceivedFragmentCount         = 10
dot11MulticastReceivedFrameCount   = 11
dot11FCSErrorCount                = 12
dot11TransmittedFrameCount         = 13
```

Related Commands

show client ccx stats-report

config client ccx test-abort

To send a request to the client to abort the current test, use the **config client ccx test-abort** command.

config client ccx test-abort *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

None.

Usage Guidelines

Only one test can be pending at a time.

Examples

```
> config client ccx test-abort 11:11:11:11:11:11
```

Related Commands

config client ccx default-gw-ping
 config client ccx dhcp
 config client ccx dns-ping
 config client ccx dns-resolve
 config client ccx test-association
 config client ccx test-dot1x
 config client ccx test-profile
 config client ccx clear-results
 config client ccx send-message
 show client ccx last-test-status
 show client ccx last-response-status
 show client ccx results
 show client ccx frame-data

config client ccx test-association

To send a request to the client to perform the association test, use the **config client ccx test-association** command.

config client ccx test-association *client_mac_address* *ssid* *bssid* **802.11{a | b | g}** channel

Syntax Description

<i>client_mac_address</i>	Specifies the MAC address of the client.
<i>ssid</i>	Network name.
<i>bssid</i>	Basic ssid.
802.11{a b g}	802.11a, 802.11b, or 802.11g setting.

Defaults

None

Examples

```
> config client ccx test-association 00:E0:77:31:A3:55 ssid bssid 802.11a
```

Related Commands

```
config client ccx default-gw-ping
config client ccx dhcp
config client ccx dns-ping
config client ccx dns-resolve
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data
```

config client ccx test-dot1x

To send a request to the client to perform the 802.1x test, use the **config client ccx test-dot1x** command.

config client ccx test-dot1x *client_mac_address profile_id bssid 802.11{a | b | g} channel*

Syntax Description

<i>client_mac_address</i>	Specifies the MAC address of the client.
<i>profile_id</i>	Specifies the test profile name.
<i>bssid</i>	Basic ssid.
802.11{a b g}	802.11a, 802.11b, or 802.11g setting.

Defaults

None.

Examples

```
> config client ccx test-dot1172.19.28.40 profile_01 bssid 802.11b
```

Related Commands

config client ccx default-gw-ping
 config client ccx dhcp
 config client ccx dns-ping
 config client ccx dns-resolve
 config client ccx test-association
 config client ccx test-profile
 config client ccx test-abort
 config client ccx clear-results
 config client ccx send-message
 show client ccx last-test-status
 show client ccx last-response-status
 show client ccx results
 show client ccx frame-data

config client ccx test-profile

To send a request to the client to perform the profile redirect test, use the **config client ccx test-profile** command.

config client ccx test-profile *client_mac_address* *profile_id*

Syntax Description	<i>client_mac_address</i>	Specifies the MAC address of the client.
	<i>profile_id</i>	Specifies the test profile name.
	Note	The <i>profile_id</i> should be from one of the client profiles for which client reporting is enabled.

Defaults None.

Examples

```
> config client ccx test-dot1 11:11:11:11:11:11 profile_01
```

Related Commands

- config client ccx default-gw-ping
- config client ccx dhcp
- config client ccx dns-ping
- config client ccx dns-resolve
- config client ccx test-association
- config client ccx test-dot1x
- config client ccx test-abort
- config client ccx clear-results
- config client ccx send-message
- show client ccx last-test-status
- show client ccx last-response-status
- show client ccx results
- show client ccx frame-data

config client deauthenticate

To disconnect a client, use the **config client deauthenticate** command.

config client deauthenticate *MAC*

Syntax Description	config	Configuration settings.
	client	Network client.
	deauthenticate	Deauthenticate command.
	<i>MAC</i>	Client MAC address.

Defaults	None.

Examples	> config client deauthenticate 11:11:11:11:11:11

Related Commands	show client summary show client detail

config client location-calibration

This command is used to configure link aggregation.

config client location-calibration [**enable** mac_address interval | **disable** mac_address]

Syntax Description	enable	Specifies that client location calibration is enabled.
	disable	Specifies that client location calibration is disabled.
	<i>mac_address</i>	Specifies the MAC address of the client.
	<i>interval</i>	Specifies the measurement interval in seconds.

Defaults None.

Examples > **config client location-calibration enable 37:15:86:2a:Bc:cf 45**

Related Commands **show client location-calibration summary**

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	config	Configuration settings.
	coredump	Controller crash file settings.
	enable disable	Enable or disable this command.

Command Default None.

Examples > 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	config	Configuration settings.
	coredump	Controller crash file settings.
	ftp	File Transfer Protocol (FTP) settings.
	<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	To configure the controller to upload a core dump file named <i>core_dump_controller</i> to an FTP server at network address <i>192.168.0.13</i> , enter this command:

```
> 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

config	Configuration settings.
coredump	Controller crash file settings.
username	Specify FTP server login information.
<i>ftp_username</i>	The FTP server login user name.
<i>ftp_password</i>	The FTP server login password.

Command Default

None.

Usage Guidelines

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

Examples

To specify a FTP server username of *admin* and password *adminpassword* for the core dump file upload, enter this command:

```
> config coredump username admin password adminpassword
```

Related Commands

[config coredump](#)
[config coredump ftp](#)
[show coredump summary](#)

config country

To configure the controller's country code, use the **config country** command. Use the **show country** command to display a list of supported countries.

config country *country_code*

Syntax Description

config	Configuration settings.
country	Set this Cisco Wireless LAN controller to comply with selected country's regulations.
<i>country_code</i>	A two-letter or three-letter country code.

Defaults

us (country code of the United States of America).

Usage Guidelines

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

Examples

```
> config country DE
```

Related Commands

show country

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	config custom-web	Command action.
	ext-webauth-mode {enable disable}	Enable or disable external URL web-based client authorization.

Defaults	None.

Examples	> 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

config custom-web	Command action.
ext-webauth-url <i>URL</i>	Set the complete external web authentication URL used for web-based client authorization.

Defaults

None.

Examples

```
> 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	config custom-web	Command action.
	ext-webserver	The URL used for web-based client authorization.
	{add delete}	Add or delete an external web server.
	<i>index</i>	Index of the external web server in the list of external web server. Must be a number between 1 and 20.
	<i>IP_address</i>	The IP address of the external web server.

Defaults None.

Examples
 > **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 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

config custom-web	Command action.
redirectUrl <i>URL</i>	Set the redirect URL to the specified address.

Defaults

None.

Examples

```
> 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

config custom-web	Command action.
internal	Set the web authentication type to internal.
customized	Set the web authentication type to customized.
external	Set the web authentication type to external.

Defaults

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

Examples

```
> 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

config custom-web	Command action.
weblogo {enable disable}	Enable or disable the web authentication logo.

Defaults

None.

Examples

```
> 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

config custom-web	Command action.
webmessage <i>message</i>	Set custom message text for web authentication.

Defaults

None.

Examples

> **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	config custom-web	Command action.
	webtitle <i>title</i>	Set the custom title text for web authentication.

Defaults	None.

Examples	<pre>> config custom-web webtitle Helpdesk</pre>

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 database size

To configure the local database, use the **config database** command. Use the **show database** command to display local database configuration.

config database size *count*

Syntax Description	config database size	Command action.
	<i>count</i>	A database size value between 512 and 2040

Defaults	None.

Examples	Configures the DHCP lease for scope 003. > config database size 1024

Related Commands	show database

config dhcp

To configure the internal DHCP, use the **config dhcp** command. Use the **show dhcp** command to display the internal DHCP configuration.

```
config dhcp { address-pool scope start end | create-scope scope |
  default-router scope router_1 [router_2] [router_3] | delete-scope scope | disable scope |
  dns-servers scope dns1 [dns2] [dns3] | domain scope domain |
  enable scope | lease scope lease_duration |
  netbios-name-server scope wins1 [wins2] [wins3] |
  network scope network netmask | opt-82 remote-id { ap_mac | ap_mac:ssid } }
```

Syntax Description	config dhcp	Command action.
	address-pool <i>scope start end</i>	Configure 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>	Create a new DHCP scope. You must specify the scope name.
	default-router <i>scope router_1 [router_2] [router_3]</i>	Configure 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>	Delete the specified DHCP scope.
	disable <i>scope</i>	Disable the specified DHCP scope.
	dns-servers <i>scope dns1 [dns2] [dns3]</i>	Configure 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>	Configure the DNS domain name. You must specify the scope and domain names.
	enable <i>scope</i>	Enable the specified dhcp scope.
	lease <i>scope lease_duration</i>	Configure the lease duration (in seconds) for the specified scope.
	netbios-name-server <i>scope wins1 [wins2] [wins3]</i>	Configure 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>	Configure the network and netmask. You must specify the scope name, the network address, and the network mask.
	opt-82 remote-id	Configure the DHCP Option 82 Remote ID Field Format.
	<i>ap_mac</i>	Adds the MAC address of the access point to the DHCP option 82 payload.
	<i>ap_mac:ssid</i>	Adds the MAC address and SSID of the access point to the DHCP option 82 payload.

Defaults None.

Examples Configures the DHCP lease for the scope 003.

```
> config dhcp lease 003
```

Related Commands

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

```
config dhcp proxy {enable | disable}
```

Syntax Description	config dhcp proxy	Command action.
	enable disable	- Enter enable to allow the controller to modify the DHCP packets without limit. - Enter disable to reduce DHCP packet modification to the level of a relay.

Defaults	Enabled.

Examples	> config dhcp proxy disable

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

config exclusionlist

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

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

Syntax Description	config exclusionlist	Configure the exclusion list.
	add delete description	- Enter add to create a local exclusion-list entry. - Enter delete to delete a local exclusion-list entry. - Enter description to set the description for an exclusion-list entry.
	MAC	MAC address of the local Excluded entry.
	description	[Optional] The description, up to 32 characters, for an excluded entry.

Defaults None.

Examples

```
> config exclusionlist add xx:xx:xx:xx:xx:xx lab
> config exclusionlist delete xx:xx:xx:xx:xx:xx lab
```

Related Commands show exclusionlist

Configure Interface Commands

Use the **config interface** commands to configure interface 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	config	Configuration settings.
	guest-lan	Guest wired LAN settings.
	create delete	Create or delete a wired LAN.
	<i>guest_lan_id</i>	A wired LAN identifier between 1 and 5 (inclusive).
	<i>interface_name</i>	Interface name up to 32 alphanumeric characters.
	enable disable	Enable or disable a wireless LAN.

Defaults None.

Examples

```
> config guest-lan enable 16
> config guest-lan create 31 foreignAp thiry1
```

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

config	Command action.
guest-lan	Configure the guest LAN.
custom-web	Customized web login page for wired guest users.
<i>ext_web_url</i>	Indicates the URL for the external server
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Defaults

None.

Examples

```
> 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

config	Command action.
guest-lan	Configure the guest LAN.
custom-web global disable	Indicates the disabling of the global custom web configuration.
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Defaults

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

```
> 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 to specify the filename of the web login page and the wired LAN for which is should display.

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

Syntax Description	config	Command action.
	guest-lan	Configure the guest LAN.
	custom-web login_page	Customized web login page for wired guest users.
	<i>page_name</i>	Indicates the name of the customized web login page.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Defaults	None.

Examples	> 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		
config		Command action.
guest-lan		Configure the guest LAN.
custom-web webauth-type		Indicates the type of web authorization page.
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).

Defaults	Internal.

Examples	> 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	config interface	Command action.
	guest-lan	Configure the guest LAN.
	ingress-interface	Provides a path between the wired guest client and the controller by way of the Layer 2 access switch.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
	<i>interface_name</i>	Interface name

Defaults None.

Examples > config interface 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		
config		Command action.
guest-lan		Configure the guest LAN.
interface		Provides a path between the wired guest client and the controller by way of the Layer 2 access switch.
<i>guest_lan_id</i>		Guest LAN identifier between 1 and 5 (inclusive).
<i>interface_name</i>		Interface name

Defaults	None.

Examples	> config guest-lan interface 1 guest01

Related Commands	config ingress-interface guest-lan config guest-lan create

config guest-lan mobility anchor

To configure guest wireless LAN settings, use the **config guest-lan mobility anchor** commands.

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

Syntax Description	config	Configuration settings.
	guest-lan	Indicates the active wired guest LAN.
	mobility anchor	Mobility anchor settings.
	add delete	Add or delete a mobility anchor.
	<i>guest_lan_id</i>	A guest LAN identifier between 1 and 5 (inclusive).
	<i>anchor_ip</i>	The IP address of the mobility anchor.

Defaults None.

Examples
 > **config guest-lan mobility anchor delete 4 192.168.0.14**

Related Commands

- 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 mobility statistics reset
- config wlan mobility anchor
- debug mobility
- show mobility anchor
- show mobility statistics
- show mobility summary

config guest-lan nac

To enable or disable NAC out-of-band support for a guest LAN, enter this command:

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

Syntax Description	config	Command action.
	guest-lan	Configure the guest LAN.
	nac	NAC out-of-band support.
	enable disable	Enable or disable NAC out-of-band support.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Defaults	None

Examples	<pre>>config guest-lan nac enable 3</pre>

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 guest_lan_id | web-passthrough enable
                             guest_lan_id }
```

Syntax Description

config	Command action.
guest-lan	Configure the guest LAN.
security	Indicates the security policy for the wired guest LAN.
guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).
web-auth enable	Enable web authentication.
web-passthrough enable	Enable the web captive portal with no authentication required.

Defaults

Web authentication.

Examples

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

Related Commands

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

config hreap group

To add, delete, or configure a hybrid-REAP group, use the **config hreap group** command.

```
config hreap group group_name {add | delete | ap {add | delete} ap-mac |  
  radius server {add | delete} {primary | secondary} server_index}
```

Syntax Description

config	Configuration settings.
hreap	Hybrid-REAP settings.
group	Hybrid-REAP group settings.
<i>group_name</i>	Enter group name.
add delete	Add or delete a hybrid-REAP group.
ap	Add or delete an access point to a hybrid-REAP group.
<i>ap-mac</i>	MAC address of the access point.
radius server	Configure a primary or secondary RADIUS server for a hybrid-REAP group.
primary secondary	Designate a RADIUS server as primary or secondary.
<i>server_index</i>	RADIUS server index number.

Defaults

None.

Usage Guidelines

You can add up to 100 clients.

Examples

```
> config hreap group 192.12.1.2 add  
> config hreap group 192.12.1.2 radius server add primary 1  
> config hreap group 192.12.1.2 ap add 00:E0:77:31:A3:55
```

Related Commands

[config ap mode](#)
[config hreap join min-latency](#)
[config hreap office-extend](#)
[debug hreap group](#)
[show hreap group detail](#)
[show hreap group summary](#)

config hreap join min-latency

To enable or disable the access point to choose the controller with the least latency when joining, use the **config hreap join min-latency** command.

config hreap join min-latency {enable | disable} *Cisco_AP*

Syntax Description

config	Configuration settings.
hreap	Hybrid-REAP settings.
join	Latency base join mode.
min-latency {enable disable}	Enable or disable the access point to choose the controller with the least latency when joining.
<i>Cisco_AP</i>	Cisco lightweight access point.

Defaults

The default value is disabled.

Usage Guidelines

When you enable this feature, the access point calculates the time between discovery request and discovery response and joins the 5500 series controller that responds first.

Examples

```
> config hreap join min-latency enable CISCO_AP
```

Related Commands

[config ap mode](#)
[config hreap group](#)
[config hreap office-extend](#)

config hreap office-extend

To configure an OfficeExtend access point, use the **config hreap office-extend** command.

```
config hreap office-extend {{enable | disable} Cisco_AP | clear-personalssid-config Cisco_AP }
```

Syntax Description	config	Configuration settings.
	hreap	Hybrid-REAP settings.
	office-extend {enable disable}	Enable or disable OfficeExtend mode for this access point.
	clear-personalssid-config	Clear only the access point's personal SSID
	<i>Cisco_AP</i>	Cisco lightweight access point.

Defaults OfficeExtend mode is enabled automatically when you enable hybrid REAP mode on the access point.

Usage Guidelines

Currently, only Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 series controller with a WPlus license can be configured to operate as OfficeExtend access points.

Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. OfficeExtend access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. You can enable or disable rogue detection for a specific access point or for all access points using this command: **config rogue detection {enable | disable} {Cisco_AP | all}**.

DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point or for all access points using this command: **config ap link-encryption {enable | disable} {Cisco_AP | all}**.

Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point using this command: **config ap telnet {enable | disable} Cisco_AP** or **config ap ssh {enable | disable} Cisco_AP**.

Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point or for all access points currently associated to the controller using this command: **config ap link-latency {enable | disable} {Cisco_AP | all}**.

Examples

```
> config hreap office-extend enable CISCO_AP
> config hreap office-extend clear-personalssid-config CISCO_AP
```

Related Commands

- [config ap mode](#)
- [config hreap join min-latency](#)
- [config hreap group](#)
- [debug hreap group](#)
- [show hreap group detail](#)
- [show hreap group summary](#)

config interface acl

To configure an interface’s Access Control List, use the **config interface acl** command.

```
config interface acl {ap-manager | management | interface_name} {ACL | none}
```

Syntax Description	config interface acl	Command action
	ap-manager	Configures the access point manager interface.
	management	Configures the management interface.
	interface_name	Enter interface name.
	{ACL none}	Specify an ACL name up to 32 alphanumeric characters or enter none.

Defaults None.

Usage Guidelines For a Cisco 2100 series wireless LAN controller, you must configure a pre-authentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any pre-authentication ACL for Cisco 4400 series wireless LAN controllers.

Examples > config interface acl management none

Related Commands show interface

config interface address

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

```

config interface address
  { ap-manager IP_address netmask gateway |
    management IP_address netmask gateway |
    service-port IP_address netmask |
    virtual IP_address |
    interface-name interface-name IP_address netmask gateway }

```

Syntax Description		
ap-manager		Specifies the access point manager interface.
management		Specifies the management interface.
service-port		Specifies the out-of-band service port interface.
virtual		Specifies the virtual gateway interface.
interface-name		Specifies the interface identified by the <i>interface-name</i> parameter.
<i>interface-name</i>		Specifies the interface name.
<i>IP_address</i>		Specifies the IP address.
<i>netmask</i>		Specifies the network mask.
<i>gateway</i>		Specifies the IP address of the gateway.

Defaults None.

Usage Guidelines For 5500 series controllers, you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

Examples > **config interface address ap-manager 10.109.15.7 255.255.0.0 10.109.15.1**

Related Commands show interface

config interface ap-manager

To enable or disable access point manager features on the management or dynamic interface, use the **config interface ap-manager** command.

```
config interface ap-manager {managemnt | interface_name} {enable | disable}
```

Syntax Description	config interface	Command action.
	ap-manager	Configures access point manager features on a dynamic interface.
	managemnt	Management interface.
	interface_name	Dynamic interface name.
	{enable disable}	Enable or disable access point manager features on a dynamic interface.

Defaults None.

Usage Guidelines

Use the **management** option to enable or disable dynamic AP management for the management interface. For 5500 series controllers, the management interface acts like an AP-manager interface by default. If desired, you can disable the management interface as an AP-manager interface and create another dynamic interface as an AP manager.

When you enable this feature for a dynamic interface, the dynamic interface is configured as an AP-manager interface (only one AP-manager interface is allowed per physical port). A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

Examples

```
> config interface ap-manager myinterface disable
```

Related Commands

show interface

config interface create

To create a dynamic interface (VLAN) for wired guest user access, use the **config interface create** command.

config interface create *interface_name* *vlan-id*

Syntax Description	config interface	Command action
	create	Create a new dynamic interface.
	<i>interface_name</i>	Interface's name.
	<i>vlan-id</i>	VLAN identifier.

Defaults	None.

Examples	> config interface create lab2 6

Related Commands	show interface

config interface delete

To delete a dynamic interface, use the **config interface delete** command.

config interface delete *interface-name*

Syntax Description	config interface	Command action.
	delete	Delete the specified dynamic interface.
	<i>interface-name</i>	Interface's name.

Defaults	None.

Examples	> config interface delete VLAN501

Related Commands	show interface

config interface dhcp

To configure DHCP options on an interface, use the **config interface dhcp** command.

```
config interface dhcp {
  ap-manager [primary dhcp_server secondary dhcp_server | option-82 [enable | disable] ] |
  management [primary dhcp_server secondary dhcp_server | option-82 [enable | disable] ] |
  service-port {enable | disable} |
  dynamic interface name [primary dhcp_server secondary dhcp_server | option-82 [enable |
  disable] ] }
```

Syntax Description

ap-manager	Configures the access point manager interface.
server-1	Configures the primary DHCP server.
<i>dhcp_server</i>	Specifies the IP address of the server.
server-2	Configures the alternate DHCP server.
option-82	Configures DHCP option 82 on the interface.
enable	Enables the feature.
disable	Disables the feature.
management	Configures the management interface.
service-port	Enables or disables DHCP for the out-of-band service port.
dynamic interface	Enter the interface name and the primary DHCP server. Optionally, you can also enter the address of the alternate DHCP server.

Defaults

None.

Examples

```
> config interface dhcp ap-manager server-1 10.21.15.01 server-2 10.21.15.25
> config interface dhcp ap-manager option-82 enable
> config interface dhcp service-port enable
```

Related Commands

[config dhcp](#)
[config dhcp proxy](#)
[config interface dhcp](#)
[config wlan dhcp_server](#)
[debug dhcp](#)
[debug dhcp service-port](#)
[debug disable-all](#)
[show dhcp](#)
[show dhcp proxy](#)
[show interface](#)

config interface guest-lan

To enable or disable the guest LAN VLAN, use the **config interface guest-lan** command.

```
config interface guest-lan interface_name {enable | disable}
```

Syntax Description	config interface	Command action.
	guest-lan	Configure the guest LAN.
	interface_name	Interface name.
	enable disable	Enable or disable the feature.

Defaults None.

Examples > config interface guest-lan myinterface enable

Related Commands config guest-lan create

config interface hostname

To configure the DNS host name of the virtual gateway interface, use the **config interface hostname** command.

```
config interface hostname virtual DNS_host
```

Syntax Description	config interface	Command action.
	hostname	Configure the DNS host name
	virtual <i>DNS_host</i>	Configures the virtual gateway interface to use the specified virtual address of the fully qualified DNS name.
		(The Virtual Gateway IP Address is any fictitious, unassigned IP address, such as 1.1.1.1, to be used by Layer 3 security and mobility managers.)

Defaults	None.

Examples	> config interface hostname virtual DNS_Host

Related Commands	show interface

config interface nat-address

To deploy your 5500 series controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT), use the **config interface nat-address** command.

```
config interface nat-address {management | dynamic-interface interface_name} {{enable |
disable} | {set public_IP_address}}
```

Syntax Description

config interface	Command action.
nat-address	NAT
management	Management interface.
dynamic-interface <i>interface_name</i>	Dynamic interface name.
enable disable	Enable or disable one-to-one mapping NAT on the interface.
set <i>public_IP_address</i>	Set the external NAT IP address.

Defaults

None.

Usage Guidelines

These NAT commands can be used only on 5500 series controllers and only if the management interface is configured for dynamic AP management.

These commands are supported for use only with one-to-one-mapping NAT, whereby each private client has a direct and fixed mapping to a global address. They do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

Examples

```
> config interface nat address management enable
> config interface nat address management set 10.10.10.10
```

Related Commands

show interface

config interface port

To map a physical port to the interface (if a link aggregation trunk is not configured), use the **config interface port** command.

```
config interface port {management | interface_name} primary_port {secondary_port}
```

Syntax Description	config interface port	Command action.
	management	Management interface.
	<i>interface_name</i>	Interface name.
	<i>primary_port</i>	Interface’s primary or (optional) secondary physical port number.
	<i>secondary_port</i>	

Defaults None.

Usage Guidelines You can use the **management** option for all controllers except the 5500 series.

Examples > **config interface port lab02 3**

Related Commands **show interface**
 config interface create

config interface quarantine vlan

To configure a quarantine VLAN on any dynamic interface, use the **config interface quarantine vlan** command.

```
config interface quarantine vlan interface-name vlan_id
```

Syntax Description	config interface	Command action.
	quarantine vlan	Configure quarantine VLAN for this interface.
	interface-name	Interface's name.
	vlan_id	VLAN identifier.
	Note Enter 0 to disable quarantine processing.	

Defaults None.

Examples > config interface quarantine vlan quarantine 10

Related Commands show interface

config interface vlan

To configure an interface's VLAN identifier, use the **config interface vlan** command.

config interface vlan { **ap-manager** | **management** | *interface-name* } *vlan*

Syntax Description	config interface	Command action.
	vlan	Configure an interface's VLAN identifier
	ap-manager management <i>interface-name</i>	- Enter ap-manager to configure the access point manager interface. - Enter management to configure the management interface. - Enter the interface's name.
	<i>interface-name</i>	Interface's name.
	<i>vlan</i>	VLAN identifier.

Defaults None.

Examples > **config interface vlan management 01**

Related Commands **show interface**

config known ap

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

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

Syntax Description	config	Configuration settings.
	known ap	Known Cisco lightweight access point.
	add alert delete	• Add a new known access point Entry. • Generate a trap upon detection of the access point. • Delete an existing known access point Entry.
	MAC	MAC address of the known Cisco lightweight access point.

Defaults None.

Examples > config known ap add ac:10:02:72:2f:bf 12

Related Commands config ap

config lag

To enable or disable link aggregation (LAG), use the **config lag** command.

config lag {enable | disable}

Syntax Description	config	Configuration settings.
	lag	Link aggregation settings.
	enable disable	Enable or disable this command.

Defaults None.

Examples

```
> config lag enable

Enabling LAG will map your current interfaces setting to LAG interface,
All dynamic AP Manager interfaces and Untagged interfaces will be deleted
All WLANs will be disabled and mapped to Mgmt interface
Are you sure you want to continue? (y/n)

You must now reboot for the settings to take effect.

> config lag disable

Disabling LAG will map all existing interfaces to port 1.
Are you sure you want to continue? (y/n)

You must now reboot for the settings to take effect.
```

Related Commands **show lag summary**

config ldap

To configure lightweight directory access protocol (LDAP) server settings, use the **config ldap** command.

config ldap {**add** | **delete** | **disable** | **enable** | **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. Valid values are from 1 to 17.

Defaults

None.

Examples

```
> config ldap enable 10
```

Related Commands

[config ldap add](#)
[config ldap simple-bind](#)
[show ldap summary](#)

config ldap add

This command is used to configure a lightweight directory access protocol (LDAP) server.

config ldap add *index server_ip_address port user_base user_attr user_type*

Syntax Description		
<i>index</i>		Specifies the LDAP server index.
<i>server_ip_address</i>		Specifies the IP address of the LDAP server.
<i>port</i>		Specifies the port.
<i>user_base</i>		Specifies the distinguished name for the subtree that contains all of the users.
<i>user_attr</i>		Specifies the attribute that contains the user's name.
<i>user_type</i>		Specifies the objectType that identifies the user.

Defaults None.

Examples

```
> config ldap add 10 10.31.15.45 2 base_name attr_name type_name
```

Related Commands

- [config ldap](#)
- [config ldap simple-bind](#)
- [show ldap summary](#)

config ldap simple-bind

To configure the local authentication bind method for the LDAP server, use the **config ldap simple-bind** command.

```
config lap simple-bind {anonymous index | authenticated index username username password
                        password}
```

Syntax Description	anonymous	Allows anonymous access to the LDAP server
	<i>index</i>	Specifies the LDAP server index.
	authenticated	Requires that a username and password be entered to secure access to the LDAP server.
	username <i>username</i>	Username for authenticated bind method.
	password <i>password</i>	Password for authenticated bind method.

Defaults The dedault bind method is **anonymous**.

Examples > config ldap simple-bind anonymous

Related Commands [config ldap](#)
[config ldap add](#)
[show ldap summary](#)

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] [max-message size] [none] } } { max-session sessions } { notify {disable | url} username password }
```

Syntax Description

config	Configuration settings.
license agent	License agent settings.
default	Default license agent.
disable	Disables the feature.
authenticate	Enables authentication.
none	Disables authentication.
listener http	Configures the license agent to receive license requests from the CLM.
encrypt	Enables encryption (HTTPS).
plaintext	Disables encryption (HTTP).
<i>url</i>	Specifies the URL where the license agent receives the requests.
acl <i>acl</i>	Specifies the access control list for license requests.
max-message <i>size</i>	The maximum message size (in bytes) for license requests. The valid range is from 0 to 65535.
none	Disable authentication on customized license agent listener.
max-sessions <i>sessions</i>	Configure maximum number of sessions allowed for the license agent. The valid range is from 1 to 25.
notify	Configure the license agent to send license notifications to the CLM.
<i>url</i>	Specifies the URL where the license agent sends the notifications.
<i>username</i>	Username used in license agent notification.
<i>password</i>	Password used in license agent notification.

Defaults

License agent is **disabled** by default.

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 want to consider using the Cisco License Manager (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/go/clm>

Examples

```
> config license agent default authenticate
> 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	config	Configuration settings.
	license boot	License boot settings.
	base wplus auto	License level.

Defaults 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 > **config boot wplus**

Related Commands

- [license install](#)
- [license modify priority](#)
- [show license in-use](#)

config load-balancing

To globally configure aggressive load balancing on the controller, use the **config load-balancing** command.

config load-balancing { **aggressive** { **enable** | **disable** } | **window** *clients* | **denial** *count* }

Syntax Description

config	Configuration settings.
load-balancing	Configures aggressive load-balancing.
aggressive { enable disable }	Enable or disable the aggressive load balancing status.
window <i>clients</i>	Set the aggressive load balancing client window with the number of clients from 1 to 20.
denial <i>count</i>	Set the maximum number of association denials during load balancing, from 0 to 10.

Defaults

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.

Examples

```
> config load-balancing aggressive enable
```

Related Commands

show load-balancing

config local-auth active-timeout

To specify the amount of time in which the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fails, enter this command:

config local-auth active-timeout *timeout*

Syntax Description	config	Configuration settings.
	local-auth	Configures local authentication.
	active-timeout	The amount of time in which the controller attempts to authenticate wireless clients using local EAP.
	<i>timeout</i>	The timeout measured in seconds. Valid range is 1 to 3600.

Defaults This command has a default of 100 seconds.

Examples > **config local-auth active-timeout 500**

Related Commands

- [clear stats local-auth](#)
- [config local-auth eap-profile](#)
- [config local-auth method fast](#)
- [config local-auth user-credentials](#)
- [debug aaa local-auth](#)
- [show local-auth certificates](#)
- [show local-auth config](#)
- [show local-auth statistics](#)

config local-auth eap-profile

This command is used to configure local EAP authentication profiles.

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

Syntax Description

config	Configures parameters.
local-auth	Configures local authentication.
eap-profile	Configures a local EAP profile.
add	Specifies that an EAP profile or method is being added.
delete	Specifies that an EAP profile or method is being deleted.
cert-issuer	(For use with EAP-TLS, PEAP, or EAP-FAST with certificates) Specifies the issuer of the certificates that will be sent to the client. The supported certificate issuers are Cisco or a third-party vendor.
method	Configures an EAP profile method.
<i>method</i>	Specifies the EAP profile method name. The supported methods are leap, fast, tls, and peap.
<i>profile_name</i>	Specifies the EAP profile name (up to 63 alphanumeric characters). Do not include spaces within a profile name.
local-cert	(For use with EAP-FAST) Specifies whether the device certificate on the controller is required for authentication.
client-cert	(For use with EAP-FAST) Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.
peer-verify	Configures the peer certificate verification options.
ca-issuer	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the incoming certificate from the client is to be validated against the Certificate Authority (CA) certificates on the controller.
cn-verify	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates' CN on the controller.
date-valid	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.
enable	Specifies that the parameter is enabled.
disable	Specifies that the parameter is disabled.

Defaults

None.

Examples

To create a local EAP profile named “FAST01,” enter this command:

```
> config local-auth eap-profile add FAST01
```

To add the EAP-FAST method to a local EAP profile, enter this command:

```
> config local-auth eap-profile method add fast FAST01
```

To specify Cisco as the issuer of the certificates that will be sent to the client for an EAP-FAST profile, enter this command:

```
> config local-auth eap-profile method fast cert-issuer cisco
```

To specify that the incoming certificate from the client be validated against the CA certificates on the controller, enter this command:

```
> config local-auth eap-profile method fast peer-verify ca-issuer enable
```

Related Commands

[config local-auth active-timeout](#)
[config local-auth method fast](#)
[config local-auth user-credentials](#)
[show local-auth certificates](#)
[show local-auth config](#)
[show local-auth statistics](#)
[clear stats local-auth](#)
[debug aaa local-auth](#)

config local-auth method fast

This command is used to configure an EAP-FAST profile.

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

Syntax Description

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

Defaults

None.

Examples

```
> config local-auth method fast anon-prov disable
> config local-auth method fast authority-id 0125631177
> config local-auth method fast pac-ttl 10
> config local-auth method fast server-key 210967Fa7D4A11AA
```

Related Commands

[config local-auth active-timeout](#)
[config local-auth eap-profile](#)
[config local-auth user-credentials](#)
[show local-auth certificates](#)
[show local-auth config](#)
[show local-auth statistics](#)
[clear stats local-auth](#)
[debug aaa local-auth](#)

config local-auth user-credentials

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

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



Note

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

Syntax Description

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

Defaults

None.

Examples

```
> config local-auth user-credentials local ldap
```

Related Commands

[config local-auth active-timeout](#)
[config local-auth eap-profile](#)
[config local-auth method fast](#)
[show local-auth certificates](#)
[show local-auth config](#)
[show local-auth statistics](#)
[clear stats local-auth](#)
[debug aaa local-auth](#)

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

config	Configuration settings.
location	Cisco lightweight access point location.
add delete	- Enter add to add a location element. - Enter delete to remove 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.
enable disable	- Enter enable to enable access point location-based overrides. - Enter disable to disable access point location-based overrides.
description	Adds a description for a location element.
algorithm	Note Cisco recommends 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 rssi-average	- Enter simple to specify a faster algorithm that requires low CPU overhead but provides less accuracy. - Enter rssi-average to specify a more accurate algorithm but requires more CPU overhead.
rssi-half-life	Note Cisco recommends that you do not use or modify the config location rssi-half-life command. It is set to optimal default values. Enter rssi-half-life to configure the half-life when averaging two RSSI readings.
expiry	Note Cisco recommends that you do not use or modify the config location expiry command. It is set to optimal default values. Enter expiry to configure 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>	Specifies a time value (0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, 300 seconds).

notify-threshold	Note Cisco recommends that you do not use or modify the config location notify-threshold command. It is set to optimal default values. NMSP notification threshold for RSSI measurements.
<i>threshold</i>	Valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
interface-mapping	Add or delete a new location, wireless LAN, or interface mapping element.
add delete	- Enter add to add a new location, wireless LAN, or interface mapping element. - Enter delete to remove 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	The path loss measurement (S60) request for normal clients or calibrating clients.
client	Normal, non-calibrating clients.
<i>burst_interval</i>	The valid range is 1 to 3600 seconds, and the default value is 60 seconds.
calibrating	Calibrating clients.
uniband multiband	The associated 802.11a or 802.11b/g radio (uniband) or on the associated 802.11a/b/g radio (multiband).

Defaults

Refer to Syntax Description for default values of individual arguments and keywords.

Examples

To specify the **simple** algorithm for averaging RSSI and SNR values on a location-based controller, use this command:

```
> 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	config	Configuration settings.
	logging	Syslog facility logging.
	buffered	Controller buffer.
	security_level	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

Defaults	None.

Examples	> 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	
config	Configuration settings.
logging	Syslog facility logging.
console	Controller console.
<i>security_level</i>	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

Defaults None.

Examples > **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

config	Configuration settings.
logging	Syslog facility logging.
debug	Set debug message logging parameters.
buffered	Save debug messages to the controller buffer.
console	Save debug messages to the controller console.
syslog	Save debug messages to the syslog server.
{enable disable}	- Enter enable to enable logging of debug messages. - Enter disable to disable logging of debug messages.

Command Default

The **console** command is enabled,
The **buffered** and **syslog** commands are disabled.

Examples

```
>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	config	Configuration settings.
	logging	Syslog facility logging.
	fileinfo	Information about the source file
	{enable disable}	- Enter enable to include information about the source file in the message logs. - Enter disable to prevent the controller from displaying information about the source file in the message logs.

Defaults	None.

Examples	> 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	config	Configuration settings.
	logging	Syslog facility logging.
	procinfo	Process information.
	{enable disable}	- Enter enable to include process information in the message logs. - Enter disable to prevent the controller from displaying process information in the message logs.

Defaults	None.

Examples	> 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	config	Configuration settings.
	logging	Syslog facility logging.
	traceinfo	Traceback information.
	{enable disable}	- Enter enable to include traceback information in the message logs. - Enter disable to prevent the controller from displaying traceback information in the message logs.

Defaults None.

Examples `> 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	config	Configuration settings.
	logging	Syslog facility logging.
	syslog	System logs.
	host	Remote host.
	IP_address	IP address for the remote host.

Defaults None.

Usage Guidelines To remove a remote host that was configured for sending syslog messages, enter this command: **config logging syslog host host_IP_address delete**.

Examples > config logging syslog host 10.92.125.51

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	
config	Configuration settings.
logging	Syslog facility logging.
syslog	System logs.
facility	Syslog facility
<i>facility_code</i>	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.

Defaults None.

Examples

> 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

config	Configuration settings.
logging	Syslog facility logging.
syslog	System logs.
level	Syslog message severity level
<i>severity_level</i>	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

Defaults

None.

Examples

```
> 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 session(s), use the **config loginsession close** command.

```
config loginsession close {session_id | all}
```

Syntax Description	config	Configuration settings.
	loginsession close	Close specified telnet sessions.
	session_id all	- Enter the ID of the session to close. - Enter all to close all telnet sessions.

Defaults	None.

Examples	> config loginsession close all

Related Commands	show loginsession

Configure Macfilter Commands

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

config macfilter

To create or delete a MAC filter entry on the Cisco Wireless LAN controller, use the **config mac filters** command.

```
config macfilter {add client_MAC wlan_id [interface_name] [description] [macfilter_IP] |  
                  delete client_MAC}
```

Syntax Description		
config		Configuration settings.
macfilter		MAC address filter settings.
<i>client_MAC</i>		Client MAC address.
<i>wlan_id</i>		Wireless LAN Identifier with which the MAC filter entry should associate. A zero value associates the entry with any wireless LAN.
<i>interface_name</i>		Name of the interface. Enter 0 to specify no interface.
<i>description</i>		(Optional) Short description of the interface (up to 32 characters), in double quotes.
	Note	Description is mandatory if <i>macfilterIP</i> is specified.
<i>macfilter_IP</i>		(Optional) Specifies the IP address of the local MAC filter database.
add delete		Add or delete a MAC filter entry on the controller.

Defaults None.

Usage Guidelines Use the **config macfilter add** command to add a client locally to a wireless LAN on the Cisco Wireless LAN controller. This filter bypasses the RADIUS authentication process.

Examples

```
> config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51  
  
> config macfilter delete 11:11:11:11:11:11  
  
Deleted user 111111111111
```

Related Commands

- [show macfilter](#)
- [config macfilter ip-address](#)

config macfilter description

Use to add a description to a MAC filter, use the **config macfilter description** command.

```
config macfilter description MAC [description]
```

Syntax Description	config	Configuration settings.
	macfilter	Local MAC address filter.
	description	Sets the description for a mac filter.
	MAC	Client MAC address.
	description	Optional description within double quotes (up to 32 characters).

Defaults	None.

Examples	> config macfilter description 11:11:11:11:11:11 "MAC Filter 01"

Related Commands	show macfilter

config macfilter interface

Use to create a MAC filter client interface, use the **config macfilter interface** command.

config macfilter interface *MAC interface*

Syntax Description	config	Configuration settings.
	macfilter	Local MAC address filter.
	interface	Create interface.
	<i>MAC</i>	Client MAC address.
	<i>interface</i>	Interface's name. A value of zero is equivalent to no name.

Defaults	None.

Examples	> config macfilter interface 11:11:11:11:11:11 Lab01

Related Commands	show macfilter

config macfilter ip-address

To assign an IP address to an existing MAC filter entry, if one was not assigned using the **config macfilter add** command, use the following command:

```
config macfilter ip-address MAC_address IP_address
```

Syntax Description

config	Configuration settings.
macfilter	Local MAC address filter.
ip-address	MAC filter IP address assignment settings.
<i>MAC_address</i>	Client MAC address.
<i>IP_address</i>	Specifies the IP address for a specific MAC address in the local MAC filter database.

Defaults

None.

Examples

```
config macfilter ip-address 00:E0:77:31:A3:55 10.92.125.51
```

Related Commands

[show macfilter](#)
[config macfilter](#)

config macfilter mac-delimiter

To set the MAC delimiter (colon, hyphen, none, and single-hyphen) for MAC addresses sent to RADIUS servers, use the **config macfilter mac-delimiter** command.

config macfilter mac-delimiter { none | colon | hyphen | single-hyphen }

Syntax Description

config	Configuration settings.
macfilter	Local MAC address filter.
mac-delimiter	Configure MAC address format for RADIUS servers.
none colon hyphen single-hyphen	- Enter none to disable delimiters (for example, xxxxxxxxxx). - Enter colon to set the delimiter to colon (for example, xx:xx:xx:xx:xx:xx). - Enter hyphen to set the delimiter to hyphen (for example, xx-xx-xx-xx-xx-xx). - Enter single-hyphen to set the delimiter to a single hyphen (for example, xxxxxx-xxxxxx).

Defaults

The default delimiter is hyphen.

Examples

To have the operating system send MAC addresses to the RADIUS server in the form aa:bb:cc:dd:ee:ff:

```
> config macfilter mac-delimiter colon
```

To have the operating system send MAC addresses to the RADIUS server in the form aa-bb-cc-dd-ee-ff:

```
> config macfilter mac-delimiter hyphen
```

To have the operating system send MAC addresses to the RADIUS server in the form aabbccddeeff:

```
> config macfilter mac-delimiter none
```

Related Commands

[show macfilter](#)

config macfilter radius-compat

Use to configure the Cisco Wireless LAN controller for compatibility with selected RADIUS servers.

```
config macfilter radius-compat { cisco | free | other }
```

Syntax Description	config	Configuration settings.
	macfilter	Local MAC address filter.
	radius-compat	Compatibility with selected RADIUS server.
	cisco free other	- Enter cisco to configure Cisco ACS Compatibility mode (password is the MAC address of the server). - Enter free to configure Free RADIUS Server Compatibility mode (password is secret). - Enter other to configure for other server behaviors (no password necessary).

Defaults Other.

Examples > config macfilter radius-compat other

Related Commands [show macfilter](#)

config macfilter wlan-id

To modify a wireless LAN ID for a MAC filter, use the **config macfilter wlan-id** command.

config macfilter wlan-id *MAC wlan_id*

Syntax Description	config	Configuration settings.
	macfilter	Local MAC address filter
	wlan-id	Modify client wireless LAN ID.
	<i>MAC</i>	Client MAC address
	<i>wlan_id</i>	Wireless LAN Identifier to associate with. A value of zero is not allowed.

Defaults None.

Examples

```
> config macfilter wlanid 11:11:11:11:11:11 2
```

Related Commands [show macfilter](#)
[show wlan](#)

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, enter this command:

config memory monitor errors {enable | disable}



Note 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

config	Configuration settings.
memory	Cisco Wireless LAN Controller memory settings.
monitor	Configure memory monitoring.
errors	Configure memory error and leak monitoring.
enable disable	Enable or disable this command.

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, and you are collecting troubleshooting information.

Examples

To enable monitoring for memory errors and leaks for a controller, enter this command:

```
> 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, enter this command:

config memory monitor leaks *low_thresh high_thresh*



Note 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

config	Configuration settings.
memory	Cisco Wireless LAN Controller memory settings.
monitor	Configure memory monitoring.
leaks	Configure the auto-leak analysis.
<i>low_thresh</i>	A value in KB indicating the value below which free memory cannot fall without crashing. This value cannot be set lower than 10000KB.
<i>high_thresh</i>	A value in KB indicating the value below which the controller enters auto-leak-analysis mode. See Usage Guidelines.

Command Default

Default value for *low_thresh* is 10000KB; Default value for *high_thresh* is 30000KB.



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, and you are collecting troubleshooting information.

Default value for *low_thresh* is 10000KB; Default value for *high_thresh* is 30000KB.

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

To set the threshold values for auto-leak-analysis mode to 12000KB for the low threshold and 35000KB for the high threshold, enter this command:

```
> config memory monitor leaks 12000 35000
```

Related Commands

[config memory monitor errors](#)
[debug memory](#)
[show memory monitor](#)

Configure Mesh Commands

Use **configure mesh** commands to set mesh access point settings.

config mesh alarm

To configure alarm settings for outdoor mesh access points, use the **config mesh alarm** command.

config mesh alarm { **max-hop** | **max-children** | **low-snr** | **high-snr** | **association** | **parent-change count** } *value*

Syntax Description		
config		Configuration settings.
mesh		Mesh access point settings (indoor and outdoor).
alarm		Alarm settings for mesh access points.
max-hop <i>value</i>		Set maximum number of hops before triggering an alarm for traffic over the mesh network. Valid values are 1-16, inclusive.
max-children <i>value</i>		Set maximum number of mesh access points (MAPs) that can be assigned to a mesh router access point (RAP) before triggering an alarm. Valid values are 1-16, inclusive.
low-snr <i>value</i>		Set the low-end signal-to-noise ratio (SNR) value before triggering an alarm. Valid values are 1 to 30, inclusive.
high-snr <i>value</i>		Set the high-end SNR value before triggering an alarm. Valid values are 1 to 30, inclusive.
association <i>value</i>		Set the mesh alarm association count value before triggering an alarm. Valid values are 1 to 30, inclusive.
parent-change count <i>value</i>		Set the number of times a MAP can change its RAP association before triggering an alarm. Valid values are 1 to 30, inclusive.
<i>value</i>		Trigger value above or below which an alarm is generated. Valid values vary for each sub-command.

Defaults

See Syntax Description for command and argument value ranges.

Examples

To set the maximum hops threshold to 8, enter this command:

```
config mesh alarm max-hop 8
```

To set the upper SNR threshold to 25, enter this command:

```
config mesh high-snr value 25
```

Related Commands

[config mesh client-access](#)
[config mesh ethernet-bridging vlan-transparent](#)
[config mesh full-sector-dfs](#)
[config mesh multicast](#)
[config mesh radius-server](#)
[config mesh security](#)
[show mesh ap](#)
[show mesh security-stats](#)
[show mesh stats](#)
[show mgmtuser](#)

config mesh astools

To globally enable or disable the anti-stranding feature for outdoor mesh access points, use the **config mesh astools** command.

```
config mesh astools {enable | disable}
```

Syntax Description	config	Configuration settings.
	mesh	Mesh access point settings (indoor and outdoor).
	astools	Global anti-stranding feature for outdoor mesh access points.
	enable disable	Enable or disable this feature for all outdoor mesh access points.

Defaults None.

Examples To enable anti-stranding on all outdoor mesh access points, enter this command:
> config mesh astools enable

Related Commands [config mesh security](#)
[show mesh ap](#)
[show mesh astools stats](#)
[show mesh config](#)
[show mesh stats](#)
[show mgmtuser](#)

config mesh background-scanning

To globally enable or disable background scanning for Cisco 1510 (SkyCaptain) access points, use the **config mesh background-scanning** command.

config mesh background-scanning {enable | disable}

Syntax Description	config	Configuration settings.
	mesh	Mesh access point settings (indoor and outdoor).
	background-scanning	Global background scanning feature for outdoor mesh access points.
	enable disable	Enable or disable this feature for all outdoor mesh access points.

Defaults Disabled.

Usage Guidelines		
	Note	This is a legacy command of the Cisco 1510 (SkyCaptain) access points. The command still exists on the controller, but it is not supported on current mesh access points.

Examples To disable background scanning for all outdoor mesh access points, enter this command:

```
> config mesh background-scanning disable
```

Related Commands

- [show mesh config](#)
- [show mesh stats](#)
- [show mgmtuser](#)

config mesh backhaul rate-adapt

To globally configure the backhaul client access (universal access) settings for indoor and outdoor mesh access points, use the **config mesh backhaul** command.

config mesh backhaul rate-adapt {all | bronze | silver | gold | platinum} {enable | disable}

Syntax Description

config	Configuration settings.
mesh	Mesh access point settings (indoor and outdoor).
backhaul	Global backhaul client access feature for mesh access points.
rate-adapt	Set client access privileges for all mesh access points.
all bronze silver gold platinum	- Enter all to grant <i>universal access</i> privileges on mesh access points. - Enter bronze to grant <i>background-level</i> client access privileges on mesh access points. - Enter silver to grant <i>best effort-level</i> client access privileges on mesh access points. - Enter gold to grant <i>video-level</i> client access privileges on mesh access points. - Enter platinum to grant <i>voice-level</i> client access privileges on mesh access points.
enable disable	Enable or disable this backhaul access level for mesh access points.

Defaults

Disabled.

Usage Guidelines

To use this command, mesh backhaul with client access must be enabled using the [config mesh client-access](#) command.



Note

After this feature is enabled, all mesh access points reboot.

Examples

To set the backhaul client access to the level of best-effort, enter this command:

```
> config mesh backhaul rate-adapt silver
```

Related Commands

[config mesh secondary-backhaul](#)
[show mesh ap](#)
[show mesh backhaul rate-adapt](#)
[show mesh config](#)
[show mesh secondary-backhaul](#)
[show mesh stats](#)

config mesh battery-state

To configure the battery state for 1520 series mesh access points, use the **config mesh battery-state** command.

```
config mesh battery-state { enable | disable } { all | cisco_ap }
```

Syntax Description

config	Configuration settings.
mesh	Mesh access point settings (indoor and outdoor).
battery-state	Battery-state feature for 1520 series mesh access points.
enable disable	Enable or disable battery-state for 1520 series mesh access points.
all cisco_ap	- Enter all to apply the command to all mesh access points. - Enter <i>cisco_ap</i> to apply the command to a specific mesh access point.

Defaults

Disabled.

Examples

To set the backhaul client access to the level of best-effort, enter this command:

```
> config mesh battery-state enable all
```

config mesh client-access

To enable or disable client access to the mesh backhaul on indoor and outdoor mesh access points, use the **config mesh client-access** command.

config mesh client-access {enable | disable}

Syntax Description

config	Configuration settings.
mesh	Mesh access point settings (indoor and outdoor).
client-access	Provide or deny client access to the mesh backhaul on mesh access points.
enable disable	- Choose enable to allow wireless client association over the mesh access point backhaul 802.11a radio. - Choose disable to restrict the 802.11a radio to backhaul traffic, and allows client association only over the 802.11b/g radio.

Defaults

Disabled.

Usage Guidelines

Backhaul interfaces (802.11a radios) act as primary Ethernet interfaces. Backhauls function as trunks in the network and carry all VLAN traffic between the wireless and wired network. No configuration of primary Ethernet interfaces is required.

When this feature is enabled, 1520 series (152x) mesh access points allow wireless client association over the 802.11a radio. This implies that a 152x mesh access point can carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio.

When this feature is disabled, the 152x carries backhaul traffic over the 802.11a radio and allows client association only over the 802.11b/g radio.

Examples

To enable client access to allow wireless client association over the 802.11a radio, enter this command:

```
> config mesh client-access enable
All Mesh AP will be rebooted
Are you sure you want to start? (y/N) Y
```

To restrict wireless client association to the 802.11b/g radio, enter this command:

```
> config mesh client-access disable
All Mesh AP will be rebooted
Are you sure you want to start? (Y/N) Y
Backhaul with client access is cancelled.
```

Related Commands

[config mesh secondary-backhaul](#)
[show mesh ap](#)
[show mesh client-access](#)
[show mesh config](#)
[show mesh stats](#)

config mesh ethernet-bridging vlan-transparent

To configure how a mesh access point handles VLAN tags for Ethernet bridged traffic, use the **config mesh ethernet-bridging vlan-transparent** command:

config mesh ethernet-bridging vlan-transparent {enable | disable}

Syntax Description

config	Configuration settings.
mesh	Mesh access point settings (indoor and outdoor).
ethernet-bridging	Configure mesh Ethernet bridging settings.
vlan-transparent	Configure VLAN tags for Ethernet bridge traffic.
enable disable	- Choose enable to bridge packets as if they are untagged. - Choose disable to drop all tagged packets.

Defaults

Enabled.

Usage Guidelines



Note VLAN Transparent is enabled as a default to ensure a smooth software upgrade from 4.1.192.xxM releases to release 5.2. Release 4.1.192.xxM does not support VLAN tagging.

Examples

To bridge Ethernet packets as untagged, enter this command:

```
> config mesh ethernet-bridging vlan-transparent enable
```

To drop tagged Ethernet packets, enter this command:

```
> config mesh ethernet-bridging vlan-transparent disable
```

Related Commands

[config mesh client-access](#)
[config mesh linkdata](#)
[config mesh linktest](#)
[config mesh multicast](#)
[show mesh ap](#)
[show mesh client-access](#)
[show mesh config](#)
[show mesh stats](#)

config mesh full-sector-dfs

To globally enable or disable full-sector Dynamic Frequency Selection (DFS) on mesh access points, use the **config mesh full-sector-dfs** command.

config mesh full-sector-dfs {enable | disable}

Syntax Description

config	Configuration settings.
mesh	Mesh access point settings (indoor and outdoor).
full-sector-dfs	Configure mesh full-sector DFS settings.
enable disable	Enable or disable Dynamic Frequency Selection for mesh access points.

Defaults

None.

Usage Guidelines

This command instructs the mesh sector to make a coordinated channel change on the detection of a radar signal. For example, if a mesh access point (MAP) detects radar, the MAP will notify the root access point (RAP), and the RAP will initiate a sector change.

All MAPs and the RAP belonging to that sector go to a new channel. This lowers the probability of MAPs stranding when radar is detected on the current backhaul channel, and no other valid parent is available as backup.

Each sector change causes the network to be silent for 60 seconds (as dictated by the DFS standard).

It is expected that after a half hour, the RAP will go back to the previously configured channel. This means that if radar is frequently observed on a RAP's channel, it is important to configure a different channel for that RAP, and additionally to exclude the radar affected channel at the controller.

Examples

To enable full-sector DFS on mesh access points, enter this command:

```
> config mesh full-sector-dfs enable
```

Related Commands

[config mesh alarm](#)
[config mesh background-scanning](#)
[config mesh backhaul rate-adapt](#)
[config mesh client-access](#)
[config mesh linkdata](#)
[config mesh linktest](#)
[config mesh range](#)
[show mesh ap](#)
[show mesh security-stats](#)
[show mesh stats](#)
[show mgmtuser](#)

config mesh linkdata

To enable external MAC filtering of access points, use the **config mesh linkdata** command.

config mesh linkdata *destination_ap_name*

Syntax Description	config	Configuration settings.
	mesh	Mesh access point settings (indoor and outdoor).
	linkdata	Mesh MAC address filtering.
	<i>destination_ap_name</i>	Specifies destination access point name for MAC address filtering.

Defaults Disabled.



Usage Guidelines **Note** The **config mesh linktest** and **config mesh linkdata** commands are designed to be used together to verify information between a source and a destination access point. To get this information, first execute the **config mesh linktest** command with the access point you want link data from in the *dest_ap* argument. When the command completes, execute the **config mesh linkdata** command listing the same destination access point, and the link data will display (see example).

MAC filtering uses the local MAC filter on the controller by default.

When external MAC filter authorization is enabled, if the MAC address is not found in the local MAC filter, then the MAC address in the external RADIUS server is used.

This protects your network against rogue mesh access points by preventing access points that are not defined on the external server from joining.

Before employing external authentication within the mesh network, the following configuration is required:

- The RADIUS server to be used as an AAA server must be configured on the controller.
- The controller must also be configured on the RADIUS server.
- The mesh access point configured for external authorization and authentication must be added to the user list of the RADIUS server.

Examples

To enable external MAC address filtering on access point AP001d.710d.e300, enter these commands:

```
> config mesh linktest MAP2-1-1522.7400 AP001d.710d.e300 18 100 1000 30
```

```
LinkTest started on source AP, test ID: 0
[00:1D:71:0E:74:00]->[00:1D:71:0D:E3:0F]
```

```
Test config: 1000 byte packets at 100 pps for 30 seconds, a-link rate 18 Mb/s
```

```
In progress: | | | | | | | | | | | | | | | |
LinkTest complete
```

```
Results
=====
txPkts:                2977
```

```

txBuffAllocErr:      0
txQFullErrs:         0
Total rx pkts heard at destination:      2977
rx pkts decoded correctly:                2977
  err pkts: Total      0 (PHY 0 + CRC 0 + Unknown 0), TooBig 0, TooSmall 0
  rx lost packets:     0 (incr for each pkt seq missed or out of order)
  rx dup pkts:         0
  rx out of order:     0

avgSNR:    30, high:   33, low:    3
SNR profile      [0dB...60dB]
    0             6             0             0             0
    0             0             1             2             77
  2888           3             0             0             0
    0             0             0             0             0
  (>60dB)         0

avgNf:    -95, high:  -67, low:  -97
Noise Floor profile [-100dB...-40dB]
    0             2948           19             3             1
    0             0             0             0             0
    3             3             0             0             0
    0             0             0             0             0
  (>-40dB)        0

avgRssi:    64, high:   68, low:   63
RSSI profile      [-100dB...-40dB]
    0             0             0             0             0
    0             0             0             0             0
    0             0             0             0             0
    0             0             0             0             0
  (>-40dB)        2977

Summary PktFailedRate (Total pkts sent/recvd):      0.000%
Physical layer Error rate (Total pkts with errors/Total pkts heard): 0.000%

```

> **config mesh linkdata AP001d.710d.e300**

```

[SD:0,0,0(0,0,0), 0,0, 0,0]
[SD:1,105,0(0,0,0),30,704,95,707]
[SD:2,103,0(0,0,0),30,46,95,25]
[SD:3,105,0(0,0,0),30,73,95,29]
[SD:4,82,0(0,0,0),30,39,95,24]
[SD:5,82,0(0,0,0),30,60,95,26]
[SD:6,105,0(0,0,0),30,47,95,23]
[SD:7,103,0(0,0,0),30,51,95,24]
[SD:8,105,0(0,0,0),30,55,95,24]
[SD:9,103,0(0,0,0),30,740,95,749]
[SD:10,105,0(0,0,0),30,39,95,20]
[SD:11,104,0(0,0,0),30,58,95,23]
[SD:12,105,0(0,0,0),30,53,95,24]
[SD:13,103,0(0,0,0),30,64,95,43]
[SD:14,105,0(0,0,0),30,54,95,27]
[SD:15,103,0(0,0,0),31,51,95,24]
[SD:16,105,0(0,0,0),30,59,95,23]
[SD:17,104,0(0,0,0),30,53,95,25]
[SD:18,105,0(0,0,0),30,773,95,777]
[SD:19,103,0(0,0,0),30,745,95,736]
[SD:20,105,0(0,0,0),30,64,95,54]
[SD:21,103,0(0,0,0),30,747,95,751]
[SD:22,105,0(0,0,0),30,55,95,25]
[SD:23,104,0(0,0,0),30,52,95,35]
[SD:24,105,0(0,0,0),30,134,95,23]

```

```
[SD:25,103,0(0,0,0),30,110,95,76]  
[SD:26,105,0(0,0,0),30,791,95,788]  
[SD:27,103,0(0,0,0),30,53,95,23]  
[SD:28,105,0(0,0,0),30,128,95,25]  
[SD:29,104,0(0,0,0),30,49,95,24]  
[SD:30,0,0(0,0,0),0,0,0,0]
```

Related Commands

- [config mesh alarm](#)
- [config mesh client-access](#)
- [config mesh ethernet-bridging vlan-transparent](#)
- [config mesh linktest](#)
- [config mesh radius-server](#)
- [show mesh ap](#)
- [show mesh client-access](#)
- [show mesh config](#)
- [show mesh stats](#)

config mesh linktest

To verify client access between mesh access points, use the **config mesh linktest** command.

config mesh linktest *source_ap* {*dest_ap* | *dest_MAC*} *datarate* *packet_rate* *packet_size* *duration*

Syntax Description

config	Configuration settings.
mesh	Mesh access point settings (indoor and outdoor).
linktest	Verify client access between mesh access points.
<i>source_ap</i>	Specifies the source access point.
<i>dest_ap</i>	Specifies the destination access point.
<i>datarate</i>	- For 802.11a radios, valid values are 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps. - For 802.11b radios, valid values are 6, 12, 18, 24, 36, 54, or 100 Mbps.
<i>packet_rate</i>	Specifies the number of packets per second. Valid range is 1 through 3000, but the recommended default is 100.
<i>packet_size</i>	(Optional) Specifies the packet size in bytes. If not specified, packet size defaults to 1500 bytes.
<i>duration</i>	(Optional) Specifies the duration of the test in seconds. Valid values are 10-300 seconds, inclusive. If not specified, duration defaults to 30 seconds.

Defaults

100 packets per second, 1500 bytes, 30 second duration.



Usage Guidelines

Note The **config mesh linktest** and **config mesh linkdata** commands are designed to be used together to verify information between a source and a destination access point. To get this information, first execute the **config mesh linktest** command with the access point you want link data from in the *dest_ap* argument. When the command completes, execute the **config mesh linkdata** command listing the same destination access point, and the link data will display.

The following warning message appears when you run a linktest that might oversubscribe the link:

```
Warning! Data Rate (100 Mbps) is not enough to perform this link test on packet size
(2000bytes) and (1000) packets per second. This may cause AP to disconnect or reboot.
Are you sure you want to continue?
```

Examples

To verify client access between mesh access points *SB_MAP1* and *SB_RAP2* at *36 Mbps*, *20 fps*, *100 frame size*, and *15* second duration, enter this command:

```
>config mesh linktest SB_MAP1 SB_RAP1 36 20 100 15
```

```
LinkTest started on source AP, test ID: 0
[00:1D:71:0E:85:00]->[00:1D:71:0E:D0:0F]
```

```
Test config: 100 byte packets at 20 pps for 15 seconds, a-link rate 36 Mb/s
```

```
In progress: | | | | | | | |
LinkTest complete
```



```

Results
=====
txPkts:                290
txBuffAllocErr:        0
txQFullErrs:           0
Total rx pkts heard at destination:      290
rx pkts decoded correctly:
    err pkts: Total      0 (PHY 0 + CRC 0 + Unknown 0), TooBig 0, TooSmall 0
    rx lost packets:     0 (incr for each pkt seq missed or out of order)
    rx dup pkts:         0
    rx out of order:     0

avgSNR:   37, high:   40, low:   5
SNR profile [0dB...60dB]
    0          1          0          0          1
    3          0          1          0          2
    8          27         243         4          0
    0          0          0          0          0
    (>60dB)    0

avgNf:   -89, high:  -58, low:  -90
Noise Floor profile [-100dB...-40dB]
    0          0          0          145         126
    11         2          0          1          0
    3          0          1          0          1
    0          0          0          0          0
    (>-40dB)   0

avgRssi:   51, high:   53, low:   50
RSSI profile [-100dB...-40dB]
    0          0          0          0          0
    0          0          0          0          0
    0          0          0          0          0
    0          7         283         0          0
    (>-40dB)   0

Summary PktFailedRate (Total pkts sent/recvd):      0.000%
Physical layer Error rate (Total pkts with errors/Total pkts heard): 0.000%

```

Related Commands

[config mesh backhaul rate-adapt](#)
[config mesh client-access](#)
[config mesh full-sector-dfs](#)
[config mesh linkdata](#)
[config mesh multicast](#)
[config mesh range](#)
[config mesh secondary-backhaul](#)
[show mesh backhaul rate-adapt](#)
[show mesh client-access](#)
[show mesh config](#)
[show mesh security-stats](#)
[show mesh stats](#)

config mesh multicast

To configure multicast mode settings to manage multicast transmissions within the mesh network, use the **config mesh multicast** commands.

config mesh multicast { regular | in | in-out }

Syntax Description

config	Configuration settings.
mesh	Mesh access point settings (indoor and outdoor).
multicast	Multicast traffic settings.
regular in in-out	- Enter regular to multicast video across the entire mesh network and all its segments by bridging-enabled Root access points (RAPs) and mesh access points (MAPs). - Enter in to forward multicast video received from the Ethernet by a MAP to the RAP's Ethernet network. No additional forwarding occurs, which ensures that non-LWAPP multicasts received by the RAP are not sent back to the MAP Ethernet networks within the mesh network (their point of origin), and MAP-to-MAP multicasts do not occur because they are filtered out. - Enter in-out to configure the RAP and MAP to multicast, but each in a different manner: - If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP Ethernets, and the MAP-to-MAP packets are filtered out of the multicast. - If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks. See Usage Guidelines for more information.

Command Default

In-out mode.

Usage Guidelines

Multicast for mesh networks cannot be enabled using the controller GUI.

Mesh multicast modes determine how bridging-enabled access points mesh access points (MAPs) and root access points (RAPs)] send multicasts among Ethernet LANs within a mesh network. Mesh multicast modes manage non-LWAPP multicast traffic only. LWAPP multicast traffic is governed by a different mechanism.

You can use the controller CLI to configure three mesh multicast modes to manage video camera broadcasts on all mesh access points. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

When using **in-out** mode, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.

**Note**

If 802.11b clients need to receive CAPWAP multicasts, then multicast must be enabled globally on the controller as well as on the mesh network (using the [config network multicast global](#) command). If multicast does not need to extend to 802.11b clients beyond the mesh network, the global multicast parameter should be disabled.

Examples

To multicast video across the entire mesh network and all its segments by bridging-enabled RAPs and MAPs, enter this command:

```
> config mesh multicast regular
```

Related Commands

[config network multicast global](#)
[config mesh backhaul rate-adapt](#)
[config mesh client-access](#)
[config mesh linktest](#)
[config mesh secondary-backhaul](#)
[show mesh ap](#)
[show mesh config](#)
[show mesh stats](#)

config mesh public-safety

To enable or disable the 4.9-GHz public safety band for mesh access points, use the **config mesh public-safety** command.

config mesh public-safety {enable | disable} {all | cisco_ap}

Syntax Description

config	Configuration settings.
mesh	Mesh access point settings (indoor and outdoor).
public-safety	4.9-GHz public safety band for mesh access points.
enable disable	Enable or disable the 4.9-GHz public safety band.
all cisco_ap	- Enter all to apply the command to all mesh access points. - Enter <i>cisco_ap</i> to apply the command to a specific mesh access point.

Defaults

Disabled.

Usage Guidelines

4.9 GHz is a licensed frequency band restricted to public-safety personnel.

Examples

To enable the 4.9-GHz public safety band for all mesh access points, enter this command:

```
> show mesh public-safety enable all
```

```
4.9GHz is a licensed frequency band in -A domain for public-safety usage
Are you sure you want to continue? (y/N) y
```

Related Commands

[config mesh range](#)
[config mesh security](#)
[show mesh ap](#)
[show mesh config](#)
[show mesh public-safety](#)
[show mesh security-stats](#)
[show mesh stats](#)

config mesh radius-server

To enable or disable external authentication for mesh access points, use the **config mesh radius-server** command.

config mesh radius-server *index* {**enable** | **disable**}

Syntax Description		
config		Configuration settings.
mesh		Mesh access point settings (indoor and outdoor).
radius-server		External authentication settings for mesh access points.
<i>index</i>		The RADIUS authentication method; options are: - Enter eap to designate extensible authentication protocol (EAP) for the mesh RADIUS server setting. - Enter psk to designate pre-shared keys (PSK) for the mesh RADIUS server setting.
enable disable		Enable or disable external authentication for mesh access points.

Defaults

EAP is enabled by default.

Examples

To enable or disable external authentication for mesh access points, enter this command:

```
> config mesh radius-server eap enable
```

Related Commands

[config mesh alarm](#)
[config mesh security](#)
[show mesh ap](#)
[show mesh security-stats](#)
[show mesh stats](#)

config mesh range

To globally set the maximum range between outdoor mesh root access points (RAPs) and mesh access points (MAPs), use the **config mesh range** command.

config mesh range [*distance*]

Syntax Description

config	Configuration settings.
mesh	Mesh access point settings (indoor and outdoor).
range	Maximum range settings between RAPs and MAPs.
<i>distance</i>	Specifies the maximum operating range (150 to 132000 ft) of the mesh access point.

Defaults

12,000 feet.

Usage Guidelines

After this command is enabled, all outdoor mesh access points reboot. This command does not affect indoor access points.

Examples

To set the range between an outdoor mesh RAP and a MAP, enter this command:

```
> config mesh range 300
```

```
Command not applicable for indoor mesh. All outdoor Mesh APs will be rebooted
Are you sure you want to start? (y/N) y
```

Related Commands

[config mesh astools](#)
[config mesh background-scanning](#)
[config mesh ethernet-bridging vlan-transparent](#)
[config mesh full-sector-dfs](#)
[config mesh linkdata](#)
[config mesh linktest](#)
[show mesh ap](#)
[show mesh stats](#)

config mesh secondary-backhaul

To configure a secondary backhaul on the mesh network, use the **config mesh secondary-backhaul** command.

```
config mesh secondary-backhaul { enable [force-same-secondary-channel] |
                                disable [rll-retransmit | rll-transmit] }
```

Syntax Description	config	Configuration settings.
	mesh	Mesh access point settings (indoor and outdoor).
	secondary-backhaul	Secondary backhaul settings.
	enable	Enables the secondary backhaul configuration.
	force-same-secondary-channel	Enables secondary-backhaul Mesh capability. Forces all access points rooted at the first hop node to have the same secondary channel and ignores the automatic or manual channel assignments for the MAPs at the second hop and beyond.
	disable	Specifies the secondary backhaul configuration is disabled.
	rll-transmit rll-retransmit	- Enter rll-transmit to use RLL at the second hop and beyond. - Enter rll-retransmit to extend the number of reliable link layer (RLL) retry attempts in an effort to improve reliability.

Command Default None.

Usage Guidelines  **Note** The secondary backhaul access feature is not supported by Cisco 1520 and 1524 indoor mesh access points in the 5.2 release.

This command uses a secondary backhaul radio as a temporary path for traffic that cannot be sent on the primary backhaul due to intermittent interference.

Examples To enable a secondary backhaul radio and force all access point rooted at the first hop node to have the same secondary channel, enter this command:

```
> config mesh secondary-backhaul enable force-same-secondary-channel
```

Related Commands

- [config mesh backhaul rate-adapt](#)
- [show mesh backhaul rate-adapt](#)
- [show mesh client-access](#)
- [show mesh config](#)
- [show mesh secondary-backhaul](#)
- [show mesh stats](#)

config mesh security

To configure the security settings for mesh networks, use the **config mesh security** commands.

config mesh security { { **rad-mac-filter** | **force-ext-auth** } { **enable** | **disable** } } | **eap** | **psk** }

Syntax Description

config	Configuration settings.
mesh	Mesh access point settings (indoor and outdoor).
security	Configure security settings for mesh networks.
rad-mac-filter force-ext-auth	- Enter rad-mac-filter to enable or disable a RADIUS MAC address filter for the mesh security setting. - Enter force-ext-auth to enable or disable forced external authentication for the mesh security setting.
enable disable	Enable or disable the setting.
eap psk	- Enter eap to designate extensible authentication protocol (EAP) for the mesh security setting. - Enter psk to designate pre-shared keys (PSK) for the mesh security setting.

Command Default

EAP.

Examples

To configure EAP as the security option for all mesh access points, use this command:

```
> config mesh security eap
```

To configure PSK as the security option for all mesh access points, use this command:

```
> config mesh security psk
```

Related Commands

[config mesh alarm](#)
[config mesh background-scanning](#)
[config mesh client-access](#)
[config mesh public-safety](#)
[config mesh radius-server](#)
[show mesh ap](#)
[show mesh client-access](#)
[show mesh config](#)
[show mesh security-stats](#)
[show mesh stats](#)

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
config	Configuration settings.
mgmtuser	Management user account.
add	Add a management user account.
<i>username</i>	Account username. Up to 24 alphanumeric characters.
<i>password</i>	Account password. Up to 24 alphanumeric characters.
lobby-admin	Adds a management user of type lobby ambassodar who can create guest accounts.
read-write read-only	- Enter read-write to create a management user with read-write access. - Enter read-only to create a management user with read-only access.
<i>description</i>	Optional description of the account. Up to 32 alphanumeric characters within double quotes.

Defaults None.

Examples
 > 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	config	Configuration settings.
	mgmtuser	Management user account.
	delete	Delete a management user account.
	<i>username</i>	Account username up to 24 alphanumeric characters.

Defaults None.

Examples

```
> 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

config	Configuration settings.
mgmtuser	Management user account.
description	Add a description of the management user account.
<i>username</i>	Account username. Up to 24 alphanumeric characters.
<i>description</i>	Description of the account. Up to 32 alphanumeric characters within double quotes.

Defaults

None.

Examples

```
> 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	config	Configuration settings.
	mgmtuser	Management user account
	password	Add a management user account
	<i>username</i>	Account username. Up to 24 alphanumeric characters.
	<i>password</i>	Account password. Up to 24 alphanumeric characters.

Defaults	None.

Examples	> config mgmtuser password admin 5rTfm

Related Commands	show mgmtuser

Configure Mobility Commands

Use the **config mobility** commands to configure mobility (roaming) settings.

config mobility group anchor

To create a new mobility anchor for the WLAN or wired guest LAN, enter, use the **config mobility group anchor** command.

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

Syntax Description	config	Configuration settings.
	mobility group	Mobility group member.
	anchor	Mobility group wireless LAN anchor settings
	add delete	- Enter add to add or change a mobility anchor to a wireless LAN. - Enter delete to delete a mobility anchor from a wireless LAN.
	wlan	Wireless LAN anchor settings.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512 (inclusive).
	guest-lan	Guest LAN anchor settings.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
	<i>anchor_ip</i>	IP address of the anchor controller.

Defaults None.

Usage Guidelines The *wlan_id* or *guest_lan_id* must exist and be disabled.

Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor. Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.

Examples

```
> config mobility group anchor add wlan 2 192.12.1.5
> config mobility group anchor delete wlan 5 193.13.1.5
> config mobility group anchor add guest-lan 2 255.255.255.0
```

Related Commands

- config guest-lan mobility 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 mobility statistics reset
- config wlan mobility anchor
- debug mobility

show mobility anchor
show mobility statistics
show mobility summary

config mobility group domain

To configure the mobility domain name, use the **config mobility group domain** command.

config mobility group domain *domain_name*

Syntax Description

config	Configuration settings.
mobility group	Mobility group member.
domain	Enable or disable mobility group feature.
<i>domain_name</i>	Domain name. Up to 31 characters; case sensitive.

Defaults

None.

Examples

```
> config mobility group domain lab1
```

Related Commands

[config mobility group anchor](#)
[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 mobility statistics reset](#)
[debug mobility](#)
[show mobility anchor](#)
[show mobility statistics](#)
[show mobility summary](#)

config mobility group keepalive count

To configure the controller to detect failed mobility group members (including anchor controllers), use the **config mobility group keepalive count** commands.

config mobility group keepalive count *count*—Specifies the number of times a ping request is sent to a mobility group member before the member is considered unreachable. The valid range is 3 to 20, and the default value is 3.

Syntax Description

config	Configuration settings.
mobility group	Mobility group member.
keepalive count	Specifies the number of times a ping request is sent to a mobility group member before the member is considered unreachable.
<i>count</i>	The valide range is 3 to 20. The default is 3.

Defaults

3.

Examples

```
> config mobility group keepalive count 3
```

Related Commands

[config mobility group anchor](#)
[config mobility group domain](#)
[config mobility group keepalive interval](#)
[config mobility group member](#)
[config mobility group multicast-address](#)
[config mobility multicast-mode](#)
[config mobility secure-mode](#)
[config mobility statistics reset](#)
[debug mobility](#)
[show mobility anchor](#)
[show mobility statistics](#)
[show mobility summary](#)

config mobility group keepalive interval

To configure the controller to detect failed mobility group members (including anchor controllers), use the **config mobility group keepalive** commands.

config mobility group keepalive interval *seconds*—Specifies the amount of time (in seconds) between each ping request sent to a mobility group member. The valid range is 1 to 30 seconds, and the default value is 10 seconds.

Syntax Description	config	Configuration settings.
	mobility group	Mobility group member.
	keepalive interval	Specifies the amount of time (in seconds) between each ping request sent to a mobility group member.
	<i>interval</i>	The valid range is 1 to 30 seconds. The default value is 10 seconds.

Defaults **config mobility group keepalive interval**—10 seconds.

Examples
 > **config mobility group keepalive interval 10**

Related Commands

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

config mobility group member

To add or delete users from the mobility group member list, use the **config mobility group member** command.

config mobility group member {**add** *MAC IP_address* [*group_name*] | **delete** *MAC*}

Syntax Description

config	Configuration settings.
mobility group member	Mobility group member.
{ add delete }	- Enter add to add or change a mobility group member to the list. - Enter delete to delete a mobility group member from the list.
<i>MAC</i>	Member switch MAC address.
<i>IP_address</i>	Member switch IP address.
<i>group_name</i>	Optional member switch group name (if different from the default group name).

Defaults

None.

Examples

```
> config mobility group member add 11:11:11:11:11:11 192.12.1.2
```

Related Commands

[config mobility group anchor](#)
[config mobility group domain](#)
[config mobility group keepalive count](#)
[config mobility group keepalive interval](#)
[config mobility group multicast-address](#)
[config mobility multicast-mode](#)
[config mobility secure-mode](#)
[config mobility statistics reset](#)
[debug mobility](#)
[show mobility anchor](#)
[show mobility statistics](#)
[show mobility summary](#)

config mobility group multicast-address

You can configure the multicast group IP address for non-local groups within the mobility list. To do so, enter this command:

config mobility group multicast-address *group_name IP_address*

Syntax Description	config	Configuration settings.
	mobility group	Mobility group
	multicast-address	Multicast address
	<i>group_name</i>	Optional member switch group name (if different from the default group name).
	<i>IP_address</i>	Member switch IP address.

Defaults None.

Examples > `config mobility group multicast-address test 10.10.10.1`

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 multicast-mode](#)
- [config mobility secure-mode](#)
- [config mobility statistics reset](#)
- [debug mobility](#)
- [show mobility anchor](#)
- [show mobility statistics](#)
- [show mobility summary](#)

config mobility multicast-mode

To enable or disable multicast mobility mode, enter this command:

```
config mobility multicast-mode {enable | disable} local_group_multicast_address
```

Syntax Description	config	Configuration settings.
	mobility	Mobility multicast mode.
	multicast-mode	
	{enable disable}	- Enter enable to enable multicast mode, the controller uses multicast mode to send Mobile Announce messages to the local group - Enter disable to disable multicast mode, the controller uses unicast mode to send the Mobile Announce messages to the local group.
	local_group_multicast_address	IP address for the local mobility group

Defaults Disabled.

Examples > config mobility multicast-mode enable 157.168.20.0

- 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 secure-mode
 - config mobility statistics reset
 - debug mobility
 - show mobility anchor
 - show mobility statistics
 - show mobility summary

config mobility secure-mode

To configure the secure mode for mobility messages between Cisco Wireless LAN controllers, use the **config mobility secure-mode** command.

config mobility secure-mode {enable | disable}

Syntax Description		
config		Configuration settings.
mobility		Mobility group member.
secure-mode		Configure the secure mode for mobility messages.
enable disable		Enable or disable mobility group message security.

Defaults None.

Examples > **config mobility secure-mode enable**

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 statistics reset
- debug mobility
- show mobility anchor
- show mobility statistics
- show mobility summary

config mobility statistics reset

To reset the mobility statistics, use the **config mobility statistics** command.

config mobility statistics reset

Syntax Description

config	Configuration settings.
mobility	Mobility group.
statistics reset	Reset mobility group statistics.

Defaults

None.

Examples

```
> config mobility statistics reset
```

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](#)
[debug mobility](#)
[show mobility anchor](#)
[show mobility statistics](#)
[show mobility summary](#)

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.



Note

The message log always collects and displays critical messages, regardless of the message log level setting.

config msglog level critical

Syntax Description

config	Configuration settings.
msglog level	Configure msglog severity levels.
critical	Collect and display critical messages.

Defaults

Config msglog level error.

Examples

```
> config msglog level critical
```

```
> show msglog
```

```
Message Log Severity Level..... CRITICAL
(messages)
```

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	config	Configuration settings.
	msglog level	Configure msglog severity levels.
	error	Collect and display critical and non-critical error messages.

Defaults Config msglog level error.

Examples

```
> config msglog level error

> show msglog

Message Log Severity Level..... ERROR
(messages)
```

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

config	Configuration settings.
msglog level	Configure msglog severity levels.
security	Collect and display critical, non-critical, and authentication- or security-related errors.

Defaults

Config msglog level error.

Examples

```
> config msglog level security
```

```
> show msglog
```

```
Message Log Severity Level..... SECURITY  
(messages)
```

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	config	Configuration settings.
	msglog level	Configure msglog severity levels.
	verbose	Collect and display all messages.

Defaults Config msglog level error.

Examples

```
> config msglog level verbose

> show msglog

Message Log Severity Level..... VERBOSE
(messages)
```

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	config	Configuration settings.
	msglog level	Configure msglog severity levels.
	warning	Collect and display warning messages in addition to critical, non-critical, and authentication- or security-related errors.

Defaults	Config msglog level error.

Examples	<pre>> config msglog level warning > show msglog Message Log Severity Level..... WARNING (messages)</pre>

Related Commands	show msglog

Configure Net User Commands

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

config netuser add

To add a guest user to the local network, use the **config netuser add** command.

To add a permanent user to the local user database on the controller—**config netuser add** *username password wlan wlan_id userType permanent description description*

To add a guest user on a WLAN or wired guest LAN to the local user database on the controller—**config netuser add** *username password {wlan_id | guestlan} {wlan_id | guest_lan_id} userType guest lifetime seconds description description*



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

Syntax Description

<i>username</i>	Guest username. Up to 24 alphanumeric characters.
<i>password</i>	User password. Up to 24 alphanumeric characters.
<i>wlan_id</i>	Wireless LAN identifier assigned to the user. A zero value associates the user with any wireless LAN.
[<i>description</i>]	(Optional) Short description of user. Up to 32 characters enclosed in double-quotes.
guest	(Optional) Indicates a guest lifetime value is specified.
<i>lifetime_value</i>	Specify a lifetime value (60 to 259200 or 0) in seconds for the guest user.
Note A value of 0 indicates an unlimited lifetime.	

Defaults

None.

Examples

This example adds a permanent user named Jane to the wireless network for 1 hour:

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

This example adds a guest user named 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*



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

Syntax Description

config	Configuration settings.
netuser	Local network user.
delete	Delete a user.
<i>username</i>	Network username. Up to 24 alphanumeric characters.

Defaults

None.

Examples

```
> 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	config	Configuration settings.
	netuser	Local network user of up to 24 alphanumeric characters.
	description	Add a user description.
	username	Network username.
	description	Optional user description. Up to 32 alphanumeric characters enclosed in double quotes.

Defaults	None.

Examples	> config netuser description able1 "HQ1 Contact"

Related Commands	show netuser

config netuser guest-role apply

To apply a QoS role to a guest user, use the **config netuser guest-role apply** command.

config netuser guest-role apply *username role_name*

Syntax Description	config	Configuration settings.
	netuser	Local network user.
	guest-role	QoS role for the guest user.
	apply	Apply a QoS role to a guest user.
	<i>username</i>	User name.
	<i>role name</i>	QoS guest role name.

Defaults 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

```
> 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 QoS role for a guest user, use the **config netuser guest-role create** command.

config netuser guest-role create *role_name*

Syntax Description

config	Configuration settings.
netuser	Local network user.
guest-role	QoS role for the guest user.
create	Create a user.
<i>role name</i>	QoS guest role name.

Defaults

None.

Usage Guidelines

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

Examples

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

Related Commands

config netuser guest-role delete

config netuser guest-role delete

To delete a QoS role for a guest user, use the **config netuser guest-role delete** command.

config netuser guest-role delete *role_name*

Syntax Description	config	Configuration settings.
	netuser	Local network user.
	guest-role	QoS role for the guest user.
	delete	Delete a user.
	<i>role name</i>	QoS guest role name.

Defaults	None.

Examples	> 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

config	Configuration settings.
netuser	Local network user.
guest-role	QoS role for the guest user.
qos	Quality of service
data-rate	Rate in Kbps for TCP traffic.
average-data-rate	Average rate in Kbps for TCP traffic.
<i>role_name</i>	QoS guest role name.
<i>rate</i>	Rate for TCP traffic on a per user basis.

Defaults

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, etc.). 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

```
> 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	config	Configuration settings.
	netuser	Local network user.
	guest-role	QoS role for the guest user.
	qos	Quality of service
	data-rate	Rate in Kbps for TCP traffic.
	average-realtime-rate	Average real-time rate for UDP traffic.
	<i>role_name</i>	QoS guest role name.
	<i>rate</i>	Rate for TCP traffic on a per user basis.

Defaults 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, etc.). 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
 > 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

config	Configuration settings.
netuser	Local network user.
guest-role	QoS role for the guest user.
qos	Quality of service
data-rate	Rate in Kbps for TCP traffic.
burst-data-rate	Peak rate in Kbps for TCP traffic.
<i>role_name</i>	QoS guest role name.
<i>rate</i>	Rate for TCP traffic on a per user basis.

Defaults

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, etc.). 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

```
> 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 peak 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	config	Configuration settings.
	netuser	Local network user.
	guest-role	QoS role for the guest user.
	qos	Quality of service
	data-rate	Rate in Kbps for TCP traffic.
	burst-realtime-rate	Peak real-time rate for UDP traffic.
	<i>role_name</i>	QoS guest role name.
	<i>rate</i>	Rate for TCP traffic on a per user basis.

Defaults None.

Usage Guidelines The Burst Real-Time Rate should be greater than or equal to the Average Real-Time 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, etc.). 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

```
> 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 maxEapUserLogin

To configure the maximum number of EAP user login attempts allowed for a network user, use the **config netuser maxEapUserLogin** command.

```
config netuser maxEapUserLogin count
```

Syntax Description	count	Maximum number of login sessions for a single user. The allowed values are from 0 (unlimited) to 8.

Defaults	0 (unlimited)

Examples	> config netuser maxEapUserLogin 8

Related Commands	show netuser

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* [**per method**]

Syntax Description	config	Configuration settings.
	netuser	Local network user.
	maxUserLogin	Configure the maximum number of login sessions allowed for a network user.
	<i>count</i>	Maximum number of login sessions for a single user. The allowed values are from 0 (unlimited) to 8.

Defaults	0 (unlimited)

Examples	> 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	config	Configuration settings.
	netuser	Local network user
	password	Modify the password.
	<i>username</i>	Network username. Up to 24 alphanumeric characters.
	<i>password</i>	Network user password. Up to 24 alphanumeric characters.

Defaults	None.

Examples	> 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	config	Configuration settings.
	netuser	Local network user.
	wlan-id	Configure a wireless LAN ID for a network user.
	<i>username</i>	Network username. Up to 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.

Defaults	None.

Examples	> 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	Enable 802.3 bridging.
disable	Disable 802.3 bridging.

Defaults

Disabled.

Usage Guidelines

In controller software release 5.2, the software-based forwarding architecture for 2100-series-based controllers is being replaced with a new forwarding plane architecture. As a result, 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 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

```
> 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	config	Configuration settings.
	network	Cisco Wireless LAN controller network parameter.
	allow-old-bridge-aps	Configure an old bridge access point's ability to associate with a switch.
	{enable disable}	Enable or disable switch association.

Defaults	Enabled.

Examples	> config network allow-old-bridge-aps enable

Related Commands	show network summary

config network ap-fallback

To configure Cisco lightweight access point fallback, use the **config network ap-fallback** command.

config network ap-fallback {enable | disable}

Syntax Description	config	Configuration settings.
	network	Cisco Wireless LAN controller network parameter.
	ap-fallback	Configure Cisco lightweight access point fallback.
	{enable disable}	Enable or disable Cisco lightweight access point fallback.

Defaults	Enabled.

Examples	> 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	config	Configuration settings.
	network	Cisco Wireless LAN controller network parameter.
	ap-priority	Configure lightweight access point priority reauthentication.
	{enable disable}	Enable or disable lightweight access point priority reauthentication.

Defaults Disabled.

Examples > **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

config	Configuration settings.
network	Cisco Wireless LAN controller network parameter.
apple-talk	Configure AppleTalk bridging.
{enable disable}	Enable or disable AppleTalk bridging.

Defaults

None.

Examples

```
> config network apple-talk enable
```

Related Commands

show network summary

config network arptimeout

To set the ARP entry timeout value, use the **config network arptimeout** command.

config network arptimeout *seconds*

Syntax Description	config	Configuration settings.
	network	Cisco Wireless LAN controller network parameter.
	arptimeout	Set the ARP entry timeout value.
	<i>seconds</i>	Timeout in seconds. Minimum value is 10. Default value is 300.

Defaults	300

Examples	> 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. This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.



Note

Zero-touch configuration must be enabled for this command to work.

config network bridging-shared-secret *shared_secret*

Syntax Description

config	Configuration settings.
network	Cisco Wireless LAN controller network parameter.
bridging-shared-secret	Configure the bridging shared secret.
<i>shared_secret</i>	Bridging shared secret string. Up to ten bytes.

Defaults

Enabled.

Examples

> **config network bridging-shared-secret shhh2**

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	config	Configuration settings.
	network	Network settings.
	broadcast	Configure broadcast support.
	enable disable	Enable or disable broadcast packet forwarding.

Defaults Disabled.

Usage Guidelines This command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. It uses the multicast mode configured on the controller (using the **config network multicast mode** command) to operate.

Examples

```
> 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 SSID (Service Set Identifier) changing for mobile stations, use the **config network fast-ssid-change** command.

config network fast-ssid-change { enable | disable }

Syntax Description

config	Configuration settings.
network	Cisco Wireless LAN controller network parameter.
fast-ssid-change	Configure fast ssid on mobile stations.
enable disable	Enable or disable fast SSID changing for mobile stations.

Defaults

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

```
> 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	config	Configuration settings.
	network	Cisco Wireless LAN controller network settings.
	ip-network-binding	Validate the source IP and MAC address within client packets.
	enable disable	Enable or disable 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	> config network ip-network-binding disable	
Related Commands	None.	

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. This setting is only used upon network installation and should be disabled after the initial network configuration.



Note

Because the Master Cisco Wireless LAN controller is normally not used in a deployed network, the Master Cisco Wireless LAN controller setting is automatically disabled upon reboot or OS code upgrade.

config network master-base {enable | disable}

Syntax Description

config	Configuration settings.
network	Cisco Wireless LAN controller network settings.
master-base	Configure the Cisco Wireless LAN controller.
{enable disable}	Enable or disable a Cisco Wireless LAN controller acting as a Cisco lightweight access point default master.

Defaults

None.

Examples

> **config network master-base enable**

Related Commands

None.

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.

**Note**

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.

config network mgmt-via-wireless {enable | disable}

Syntax Description

config	Configuration settings.
network	Cisco Wireless LAN controller network settings.
mgmt-via-wireless	Configure switch management via wireless interface.
{enable disable}	Enable or disable switch management via wireless interface.

Defaults

Disabled.

Examples

```
> 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}
```



Note 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 (using the **config network multicast mode** command) to operate.

Syntax Description

config	Configuration settings.
network	Network settings.
multicast global	Configure multicast support.
{enable disable}	Enable or disable multicast global support.

Defaults

Disabled.

Examples

```
> config network multicast global enable
```

Related Commands

- show network summary
- config network broadcast
- config network multicast mode

config network multicast igmp snooping

To enable or disable IGMP snooping, use the **config network multicast igmp snooping** command.

config network multicast igmp snooping

Syntax Description	config	Configuration settings.
	network	Network settings.
	multicast	Configure multicast support.
	igmp snooping	Internet Group Multicast Protocol snooping.

Defaults None.

Examples > **config network multicast igmp snooping**

Related Commands **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

Syntax Description

config	Configuration settings.
network	Network settings.
multicast	Configure multicast support.
igmp	Internet Group Multicast Protocol.
timeout	Number of seconds between 30 and 300.

Defaults

None.

Usage Guidelines

You can enter a timeout value between 30 and 300 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

```
> config network multicast igmp timeout
```

Related Commands

config network multicast igmp snooping

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

config	Configuration settings.
network	Network settings.
multicast	Configure multicast support.
mode multicast	Sends a single copy of data to multiple receivers.

Defaults

None.

Examples

```
> 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	config	Configuration settings.
	network	Network settings.
	multicast	Configure multicast support.
	mode unicast	Sends multiple copies of data, one copy for each receiver.

Defaults	None.

Examples	> config network multicast mode unicast

Related Commands	config network multicast global config network broadcast config network multicast mode multicast

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

config	Configuration settings.
network	Network settings.
otap-mode	Configure OTAP provisioning.
{enable disable}	Enable or disable OTAP provisioning.

Defaults

Enabled.

Examples

```
> 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	config	Configuration settings.
	network	Cisco Wireless LAN controller network settings.
	rf-network-name	Set the RF-network name.
	name	RF-Network name. Up to 19 characters.

Defaults None.

Examples > config network rf-network-name travelers

Related Commands show network summary

config network secureweb

To change the state of the secure web (https = http + SSL) interface, use the **config network secureweb** command.

config network secureweb {enable | disable}

Syntax Description	config	Configuration settings.
	network	Network settings.
	secureweb	Configure the secure web interface.
	{enable disable}	Enable or disable the secure web interface.

Defaults Enabled.

Usage Guidelines This command allows users to access the controller GUI using *http://ip-address*. Web mode is *not* a secure connection.

Examples

```
> 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 Socket Layer (SSL v2 for web administration and web authentication), use the **config network secureweb cipher-option** command.

config network secureweb cipher-option {high | sslv2} {enable | disable}

Syntax Description

config	Configuration settings.
network	Network settings.
secureweb	Configure the secure web interface.
enable disable	Enable or disable the secure web interface.

Defaults

Disabled for secure web mode with increased security; **enabled** for SSL v2.



Usage Guidelines

Note The **cipher-option high** command allows users to access the controller GUI using *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.

Examples

To enable secure web mode with increased security, enter this command:

```
> config network secureweb cipher-option high enable
```

To disable SSL v2, enter this command:

```
> 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

config	Configuration settings.
network	Network settings.
ssh	Secure Shell sessions
enable disable	Allow or disallow new ssh sessions.

Defaults

Disabled.

Examples

```
> 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	config	Configuration settings.
	network	Network settings.
	telnet	Configure new telnet sessions.
	{enable disable}	Allow or disallow new telnet sessions.

Defaults Disabled.

Examples > **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. Use this command to set the idle client session duration on the Cisco Wireless LAN controller. The minimum duration is 90 seconds.

config network usertimeout *seconds*

Syntax Description	config	Configuration settings.
	network	Network settings.
	usertimeout	Configure idle session timeout.
	<i>seconds</i>	Timeout duration in seconds. Minimum value is 90. Default value is 300.

Defaults	300

Examples	> config network usertimeout 1200

Related Commands	show network summary

config network web-auth-port

To configure an additional port to be redirected for web authentication, use the **config network web-auth-port** command.

```
config network web-auth-port port
```

Syntax Description	config	Configuration settings.
	network	Network settings.
	web-auth-port	Configure an additional port to be redirected for web authentication.
	<i>port</i>	Port number.

Defaults	None.

Examples	> config network web-auth-port 1200

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	config	Configuration settings.
	network	Network settings.
	webmode	Configure web user interface access.
	{enable disable}	Enable or disable the web interface.

Defaults	Enabled.

Examples	> config network webmode disable

Related Commands	show network summary

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

config	Configuration settings.
network	Cisco Wireless LAN controller network settings.
zero-config	Configure bridge access point ZeroConfig support.
{enable disable}	Enable or disable bridge access point ZeroConfig support.

Defaults

Enabled.

Examples

```
> config network zero-config enable
```

Related Commands

show network summary

config nmsp notify-interval measurement

To modify the 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

config	Configuration settings.
nmsp notify-interval measurement	Modify the NMSP notification interval.
client	Modify the interval for clients,
rfid	Modify the interval for active RFID tags.
rogue	Modify the interval for rogue access points and rogue clients.
<i>interval</i>	Between 1 and 30 seconds

Defaults

None

Usage Guidelines



Note

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 Network Mobility Services Protocol (NMSP) to function.

Examples

```
> 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 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

config	Configuration settings.
passwd-cleartext	Password display settings.
enable disable	Enable or disable display of passwords in plain text.

Defaults

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

To enable display of passwords in plain text, enter this command:

```
> 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 pmk-cache delete

To delete an entry in the PMK cache from all Cisco Wireless LAN controllers in the mobility group, use the **config pmk-cache delete** command.

```
config pmk-cache delete {all | mac_address}
```

Syntax Description	config	Configuration settings.
	pmk-cache delete	Delete an entry in the PMK cache.
	all <i>mac_address</i>	- Enter all to delete all Cisco Wireless LAN controllers. - Enter the MAC address of the Cisco Wireless LAN controller to delete.

Defaults	None.

Examples	> config pmk-cache delete all

Related Commands	show pmk-cache

Configure Port Commands

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

config port adminmode

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

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

Syntax Description

config	Configuration settings.
port	Port settings.
adminmode	Administrative mode.
all port	- Enter all to configure all ports. - Enter the number of the port to configure.
enable disable	Enable or disable the specified ports.

Defaults

Enabled.

Examples

To disable port 8:

```
> config port adminmode 8 disable
```

To enable all ports:

```
> config port adminmode all enable
```

Related Commands

- [config port autoneg](#)
- [config port linktrap](#)
- [config port multicast appliance](#)
- [config port physicalmode](#)
- [config port power](#)
- [show port](#)
- [transfer download port](#)

config port autoneg

To configure 10/100BASE-T Ethernet ports for physical port autonegotiation, use the **config port autoneg** command.

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

Syntax Description

config	Configuration settings.
port	10/100BASE-T Ethernet.
autoneg	Configure a port's auto negotiation mode.
all <i>port</i>	- Enter all to configure all ports. - Enter the number of the port to configure.
enable disable	Enable or disable the specified ports.

Defaults

All Ports = autonegotiation enabled.

Usage Guidelines

Port autoconfiguration must be disabled before you make physical mode manual settings using the **config port physicalmode** command. Also note that the **config port autoneg** command overrides settings made using the **config port physicalmode** command.

Examples

To turn on physical port autonegotiation for all front-panel Ethernet ports:

```
> config port autoneg all enable
```

To disable physical port autonegotiation for front-panel Ethernet port 19:

```
> config port autoneg 19 disable
```

Related Commands

[config port adminmode](#)
[config port linktrap](#)
[config port multicast appliance](#)
[config port physicalmode](#)
[config port power](#)
[show port](#)
[transfer download port](#)

config port linktrap

To enable or disable the up and down link traps for a specific controller port or for all ports, use the **config port linktrap** command.

```
config port linktrap {all | port} {enable | disable}
```

Syntax Description	config	Configuration settings.
	port	Port settings.
	linktrap	Link status alert.
	all port	- Enter all to configure all ports. - Enter the port number to configure.
	enable disable	Enable or disable the specified ports.

Defaults Enabled.

Examples

To disable port 8 traps:

```
> config port linktrap 8 disable
```

To enable all port traps:

```
> config port linktrap all enable
```

Related Commands

[config port adminmode](#)
[config port autoneg](#)
[config port multicast appliance](#)
[config port physicalmode](#)
[config port power](#)
[show port](#)
[transfer download port](#)

config port multicast appliance

To enable or disable the multicast appliance service for a specific controller port or for all ports, use the **config port multicast appliance** commands.

config port multicast appliance {all | port} {enable | disable}

Syntax Description	config	Configuration settings.
	port	Port settings.
	multicast appliance	Multicast appliance service settings.
	all port	- Enter all to configure all ports. - Enter the port number to configure.
	enable disable	Enable or disable the service for the specified ports.

Defaults Enabled.

Examples To enable multicast appliance service on all ports, enter this command:

```
> config port multicast appliance all enable
```

To disable multicast appliance service on port 8, enter this command:

```
> config port multicast appliance 8 disable
```

Related Commands

- [config port adminmode](#)
- [config port autoneg](#)
- [config port linktrap](#)
- [config port physicalmode](#)
- [config port power](#)
- [show port](#)
- [transfer download port](#)

config port physicalmode

To set any or all front-panel 10/100BASE-T Ethernet ports for dedicated 10 Mbps or 100 Mbps, Half or Full Duplex operation, use the **config port physicalmode** command.

config port physicalmode {**all** | *port*} {**100h** | **100f** | **10h** | **10f**}

Syntax Description

config	Configuration settings.
port	Port settings.
physicalmode	Port physical mode.
all <i>port</i>	- Enter all to configure all ports. - Enter the number of the port to configure.
100h 100f 10h 10f	- Enter 100h for 100 Mbps/Half Duplex operation. - Enter 100f for 100 Mbps/Full Duplex operation. - Enter 10h for 10 Mbps/Half Duplex operation. - Enter 10f for 10 Mbps/Full Duplex operation.

Defaults

All Ports are set to auto negotiate.

Usage Guidelines

Note that you must disable autonegotiation using the **config port autoneg** command before manually configuring any port's physical mode. Also note that the **config port autoneg** command overrides settings made using the **config port physicalmode** command.

Examples

To set all ports to 100 Mbps/Full Duplex operation:

```
> config port physicalmode all 100f
```

To set port 20 to 100 Mbps/Half Duplex operation:

```
> config port physicalmode 20 100h
```

To set port 21 to 10 Mbps/Full Duplex operation:

```
> config port physicalmode 21 10f
```

To set port 22 to 10 Mbps/Half Duplex operation:

```
> config port physicalmode 22 10h
```

Related Commands

[config port adminmode](#)
[config port autoneg](#)
[config port linktrap](#)
[config port multicast appliance](#)
[config port power](#)
[show port](#)
[transfer download port](#)

config port power

To enable or disable Power over Ethernet (PoE) for a specific controller port or for all ports, use the **config port power** commands.

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

Syntax Description

config	Configuration settings.
port	Port settings.
power	Power over Ethernet settings.
all <i>port</i>	- Enter all to configure all ports. - Enter the port number to configure.
enable disable	Enable or disable the service for the specified ports.

Defaults

Enabled.

Examples

To enable PoE on all ports, enter this command:

```
> config port port all enable
```

To disable PoE on port 8, enter this command:

```
> config port port 8 disable
```

Related Commands

[config port adminmode](#)
[config port autoneg](#)
[config port linktrap](#)
[config port multicast appliance](#)
[config port physicalmode](#)
[show port](#)
[transfer download port](#)

config prompt

To change the CLI system prompt, use the **config prompt** command.

config prompt *prompt*

Because the system prompt is a user-defined variable, it is omitted from the rest of this documentation.

Syntax Description	config	Configuration settings.
	prompt	Change the CLI system prompt.
	<i>prompt</i>	New CLI system prompt enclosed in double quotes. Up to 31 alphanumeric characters; case sensitive.

Defaults The system prompt is configured using the startup wizard.

Examples

```
> config prompt "Cisco 4400"
(Cisco 4400)>
```

Related Commands None.

config qos average-data-rate

To define the average data rate in Kbps for TCP traffic per user, use the **config qos average-data-rate** command.

config qos average-data-rate { bronze | silver | gold | platinum } rate

Syntax Description	config qos	Command action.
	average-data-rate	Rate in Kbps for TCP traffic.
	bronze silver gold platinum	Enter one of the four supported queue names.
	<i>rate</i>	A value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Defaults	None.

Examples	> config qos average-data-rate gold 0

Related Commands	show qos description config qos burst-data-rate config qos average-realtime-rate config qos burst-realtime-rate config qos max-rf-usage

config qos average-realtime-rate

To define the average real-time data rate in Kbps for UDP traffic per user, use the **config qos average-realtime-rate** command.

```
config qos average-realtime-rate {bronze | silver | gold | platinum} rate
```

Syntax Description	config qos	Command action.
	average-realtime-rate	Average actual rate in Kbps for UDP traffic.
	{bronze silver gold platinum}	Enter one of the four supported queue names.

Defaults	None.

Examples	> config qos average-realtime-rate gold rate

Related Commands	show qos description config qos average-data-rate config qos burst-data-rate config qos burst-realtime-rate config qos max-rf-usage

config qos burst-data-rate

To define the peak data rate in Kbps for TCP traffic per user, use the **config qos burst-data-rate** command.

```
config qos burst-data-rate {bronze | silver | gold | platinum} rate
```

Syntax Description	config qos	Command action.
	burst-data-rate	Peak rate in Kbps for TCP traffic.
	{bronze silver gold platinum}	Enter one of the four supported queue names.

Defaults	None.

Examples	> config qos burst-data-rate gold 30000

Related Commands	show qos description, onfig qos average-data-rate config qos average-realtime-rate config qos burst-realtime-rate config qos max-rf-usage

config qos burst-realtime-rate

To define the average real-time data rate in Kbps for UDP traffic per user, use the **config qos burst-realtime-rate** command.

```
config qos burst-realtime-rate {bronze | silver | gold | platinum} rate
```

Syntax Description	config qos	Command action.
	burst-realtime-rate	Peak actual rate in Kbps for UDP traffic.
	{bronze silver gold platinum}	Enter one of the four supported queue names.

Defaults	None.

Examples	> config qos burst-realtime-rate gold rate

Related Commands	show qos description
	config qos average-data-rate
	config qos burst-data-rate
	config qos average-realtime-rate
	config qos max-rf-usage

config qos description

To change the profile description, use the **config qos description** command.

```
config qos description {bronze | silver | gold | platinum} description
```

Syntax Description	config qos	Command action.
	description	Configure QoS profile description.
	{bronze silver gold platinum}	Enter one of the four supported queue names.

Defaults	None.

Examples	> config qos description gold <i>description</i>

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	config qos	Command action.
	max-rf-usage	Maximum percentage of RF usage.
	{bronze silver gold platinum}	Enter one of the four supported queue names.

Defaults	None.

Examples	> 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 protocol-type/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 protocol-type** and **config qos dot1p-tag** commands.

config qos protocol-type {bronze | silver | gold | platinum} {none | dot1p}

config qos dot1p-tag {bronze | silver | gold | platinum} *dot1p_tag*

Syntax Description	config qos	Command action.
	protocol-type	Configure the QoS protocol type (bronze, silver, gold, platinum)
	dot1p-tag	Configure a QoS 802.1p tag.
	{bronze silver gold platinum}	Enter one of the four supported queue names.
	none	Enter when no specific protocol is assigned.
	dot1p	Specify a 802.1p tag.
	<i>dot1p_tag</i>	Specify a dot1p tag value of between 1 and 7.

Defaults None.

Examples

```
> config qos protocol-type silver dot1p
> config qos dot1p-tag gold 5
```

Related Commands show qos queue_length all

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	config qos	Command action.
	queue_length	Configure QoS queue length.
	{bronze silver gold platinum}	Enter one of the four supported queue names.
	length	Enter the maximum queue length value (10 to 255).

Defaults	None.

Examples	> config qos queue_length gold 12

Related Commands	show qos [bronze silver gold platinum]

Configure Radius Account Commands

Use the **config radius acct** commands to configure RADIUS account server settings.

config radius acct

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

```
config radius acct [{enable | disable | delete} index] |
  add index server_ip port {ascii | hex} secret
```

Syntax Description		
config		Configuration settings.
radius acct		RADIUS accounting server settings.
enable		Enable a RADIUS accounting server.
disable		Disable a RADIUS accounting server.
delete		Delete a RADIUS accounting server.
<i>index</i>		RADIUS server index. Controller begins search with 1.
add		Add a RADIUS accounting server. See defaults.
<i>server_ip</i>		IP address of RADIUS server.
<i>port</i>		RADIUS server's UDP port number for the interface protocols.
ascii hex		RADIUS server's secret type: ascii or hex .
<i>secret</i>		RADIUS server's secret.

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

Examples To configure a priority 1 RADIUS accounting server at *10.10.10.10* using port *1813* with a login password of *admin*, enter this command:

```
> config radius acct add 1 10.10.10.10 1813 ascii admin
```

Related Commands [show radius acct statistics](#)

config radius acct fallback-test

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

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

Syntax Description

config	Configuration settings.
radius acct	RADIUS accounting server.
fallback-test	Configure the RADIUS server fallback behavior.
mode {off passive active}	• Off disables RADIUS server fallback. • Passive causes the controller to revert to a preferable server (with a lower server index) from the available backup servers without using extraneous probe messages. The controller simply ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent. • Active causes the controller to revert to a preferable server (with a lower server index) from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller simply ignores all inactive servers for all active RADIUS requests.
username	Specifies the name to be sent in the inactive server probes.
<i>username</i>	You can enter up to 16 alphanumeric characters for the <i>username</i> argument.
interval	Specifies the probe interval value.
<i>interval</i>	Probe interval range is 180 to 3600

Defaults

Default probe interval: 300.

Examples

```
> config radius acct fallback-test mode off
> config radius acct fallback-test mode passive
> config radius acct fallback-test mode active
> config radius acct fallback-test username user_1
> config radius acct fallback-test interval 500
```

Related Commands

[config advanced probe filter](#)
[config advanced probe limit](#)
[show advanced probe](#)
[show radius acct statistics](#)

config radius acct ipsec authentication

To configure IPSec authentication for the Cisco Wireless LAN controller, use the **config radius acct ipsec authentication** command.

```
config radius acct ipsec authentication {hmac-md5 | hmac-sha1} index
```

Syntax Description	config	Configuration settings.
	radius acct	RADIUS accounting server.
	ipsec authentication	Configure IPSec authentication service.
	{hmac-md5 hmac-sha1}	- Enter hmac-md5 to enable IPSec HMAC-MD5 authentication. - Enter hmac-sha1 to IPSec HMAC-SHA1 authentication.
	index	RADIUS server index.

Defaults
None.

Examples
> config radius acct ipsec authentication hmac-md5 1

Related Commands
show radius acct statistics

config radius acct ipsec disable

To disable IPSec support for an accounting server for the Cisco Wireless LAN controller, use the **config radius acct ipsec disable** command.

config radius acct ipsec disable *index*

Syntax Description	config	Configuration settings.
	radius acct	RADIUS accounting server.
	ipsec disable	Disable IPSec support for an accounting server.
	<i>index</i>	RADIUS server index.

Defaults None.

Examples > **config radius acct ipsec disable 1**

Related Commands **show radius acct statistics**

config radius acct ipsec enable

To enable IPSec support for an accounting server for the Cisco Wireless LAN controller, use the **config radius acct ipsec enable** command.

config radius acct ipsec enable *index*

Syntax Description	config	Configuration settings.
	radius acct	RADIUS accounting server.
	ipsec enable	Enable IPSec support for an accounting server.
	<i>index</i>	RADIUS server index.

Defaults	None.

Examples	> config radius acct ipsec enable 1

Related Commands	show radius acct statistics

config radius acct ipsec encryption

To configure IPSec encryption for an accounting server for the Cisco Wireless LAN controller, use the **config radius acct ipsec encryption** command.

```
config radius acct ipsec encryption {3des | aes | des} index
```

Syntax Description

config	Configuration settings.
radius acct	RADIUS accounting server.
ipsec encryption	Configure IPSec encryption.
3des aes des	- Enter 3des to enable IPSec 3DES Encryption. - Enter aes to enable IPSec AES Encryption. - Enter des to enable IPSec DES Encryption.
index	Enter a RADIUS server index value of between 1 and 17.

Defaults

None.

Examples

```
> config radius acct ipsec encryption 3des 3
```

Related Commands

- show radius acct statistics
- show radius summary

config radius acct ipsec ike

To configure Internet Key Exchange (IKE) for the Cisco Wireless LAN controller, use the **config radius acct ipsec** command.

```
config radius acct ipsec ike {dh-group {group-1 | group-2 | group-5} |
    lifetime seconds | phase1 {aggressive | main}} index
```

Syntax	Description
config	Configuration settings.
radius acct	RADIUS accounting server.
ipsec ike	Configure IKE.
dh-group {group-1 group-2 group-5}	Configure the IKE Diffie-Hellman group. - Enter group-1 to configure DH Group 1 (768 bits). - Enter group-2 to configure DH Group 2 (1024 bits). - Enter group-5 to configure DH Group 2 (1024 bits).
lifetime seconds	Configure the IKE lifetime in seconds.
phase1 {aggressive main}	Configure the IKE Phase1 mode. - Enter aggressive to enable the aggressive mode. - Enter main to enable the main mode.
index	RADIUS server index.

Defaults None.

Examples > config radius acct ipsec ike lifetime 23 1

Related Commands show radius acct statistics

config radius acct mac-delimiter

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

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

Syntax Description

config	Configuration settings.
radius acct	Default RADIUS accounting server.
mac-delimiter	Configure a default RADIUS server for network users.
colon	Sets the delimiter to a colon (for example, xx:xx:xx:xx:xx:xx)
hyphen	Sets the delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx)
single-hyphen	Sets the delimiter to a single hyphen (for example, xxxxxx-xxxxxx)
none	Disables delimiter (for example, xxxxxxxxxxxx)

Defaults

The default delimiter is hyphen.

Examples

```
> config radius acct mac-delimiter hyphen
```

Related Commands

show radius acct statistics

config radius acct network

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

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

Syntax Description	config	Configuration settings.
	radius acct	Default RADIUS accounting server.
	network	Configure a default RADIUS server for network users.
	<i>index</i>	RADIUS server index.
	{ enable disable }	Enable or disable the server as a network user's default RADIUS Server.

Defaults	None.

Examples	> config radius acct network 1 enable

Related Commands	show radius acct statistics

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	config	Configuration settings.
	radius acct	RADIUS accounting server.
	retransmit-timeout	Configure retransmission timeout.
	<i>index</i>	RADIUS server index.
	<i>timeout</i>	Number of seconds (from 2 to 30) between retransmissions.

Defaults None.

Examples > config radius acct retransmit-timeout 5

Related Commands show radius acct statistics

Configure RADIUS Authentication Server Commands

Use the **config radius auth** commands to configure RADIUS authentication server settings.

config radius auth

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

```
config radius auth { {enable | disable | delete} index } |
  add index server_ip port {ascii | hex} secret}
```

Syntax Description		
config		Configuration settings.
radius auth		RADIUS authentication server settings.
enable		Enable a RADIUS authentication server.
disable		Disable a RADIUS authentication server.
delete		Delete a RADIUS authentication server.
<i>index</i>		RADIUS server index. Controller begins search with 1.
add		Add a RADIUS authentication server. See defaults.
<i>server_ip</i>		IP address of RADIUS server.
<i>port</i>		RADIUS server's UDP port number for the interface protocols.
ascii hex		RADIUS server's secret type: ascii or hex .
<i>secret</i>		RADIUS server's secret.

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

Examples To configure a priority 1 RADIUS authentication server at 10.10.10.10 using port 1812 with a login password of *admin*, enter this command:

```
> config radius auth add 1 10.10.10.10 1812 ascii admin
```

Related Commands [show radius auth statistics](#)

config radius auth ipsec authentication

To configure IPSec support for an authentication server for the Cisco Wireless LAN controller, use the **config radius auth ipsec authentication** command.

```
config radius auth ipsec authentication {hmac-md5 | hmac-sha1} index
```

Syntax Description	config	Configuration settings.
	radius auth	RADIUS authentication server.
	ipsec authentication	Configure IPSec authentication service.
	{hmac-md5 hmac-sha1}	- Enter hmac-md5 to enable IPSec HMAC-MD5 authentication. - Enter hmac-sha1 to IPSec HMAC-SHA1 authentication.
	index	RADIUS server index.

Defaults None.

Examples > config radius auth ipsec authentication hmac-md5 1

Related Commands show radius acct statistics

config radius auth ipsec disable

To disable IPSec support for an authentication server for the Cisco Wireless LAN controller, use the **config radius auth ipsec disable** command.

config radius auth ipsec {enable | disable} index

Syntax Description	config	Configuration settings.
	radius auth	RADIUS authentication server.
	ipsec {enable disable}	- Enter enable to enable IPSec support for an authentication server. - Enter disable to disable IPSec support for an authentication server.
	index	RADIUS server index.

Defaults	None.

Examples	<pre>> config radius auth ipsec enable 1 > config radius auth ipsec disable 1</pre>

Related Commands	show radius acct statistics

config radius auth ipsec encryption

To configure IPSec support for an authentication server for the Cisco Wireless LAN controller, use the **config radius auth ipsec** command.

config radius auth ipsec encryption {**3des** | **aes** | **des**} *index*

Syntax Description	config	Configuration settings.
	radius auth	RADIUS authentication server.
	ipsec encryption	Configure IPSec encryption.
	3des aes des	- Enter 3des to enable IPSec 3DES Encryption. - Enter aes to enable IPSec AES Encryption. - Enter des to enable IPSec DES Encryption.
	<i>index</i>	RADIUS server index.

Defaults	None.

Examples	> config radius acct ipsec encryption 3des 3

Related Commands	show radius acct statistics

config radius auth ipsec ike

To configure IKE for the Cisco Wireless LAN controller, use the **config radius auth ipsec ike** command.

```
config radius auth ipsec ike {dh-group {group-1 | group-2 | group-5} |  
    lifetime seconds | phase1 {aggressive | main}} index
```

Syntax	Description
config	Configuration settings.
radius auth	RADIUS authentication server.
ipsec ike	Configure IKE.
dh-group group-1 group-2 group-5	Configure the IKE Diffie-Hellman group. - Enter group-1 to configure DH Group 1 (768 bits). - Enter group-2 to configure DH Group 2 (1024 bits). - Enter group-5 to configure DH Group 2 (1024 bits).
lifetime <i>seconds</i>	Configure the IKE lifetime in seconds.
phase1 aggressive main	Configure the IKE Phase1 mode. - Enter aggressive to enable the aggressive mode. - Enter main to enable the main mode.
<i>index</i>	RADIUS server index.

Defaults None.

Examples > **config radius auth ipsec ike lifetime 23 1**

Related Commands show radius acct statistics

config radius auth keywrap

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

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

Syntax Description

config	Configuration settings.
radius auth	RADIUS authentication server.
keywrap	Configure AES key wrap
enable disable add	- Enter enable to enable AES key wrap. - Enter disable to disable AES key wrap. - Enter add to configure the AES key wrap attributes.
ascii hex	- Enter ascii to configure the key wrap in ascii format. - Enter hex to configure the key wrap in hexadecimal format.
kek	Specifies the 16-byte Key Encryption Key (KEK).
mack	Specifies the 20-byte Message Authentication Code Key (MACK).
index	Specifies the index of the RADIUS authentication server on which to configure the AES key wrap.

Defaults

None.

Examples

```
> config radius auth keywrap enable
> config radius auth keywrap disable
> config radius auth keywrap add ascii kek mack index
```

Related Commands

show radius auth statistics

config radius auth mac-delimiter

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

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

Syntax Description

config	Configuration settings.
radius acct	Default RADIUS authentication server.
mac-delimiter	Configure a default RADIUS server for network users.
colon	Sets the delimiter to a colon (for example, xx:xx:xx:xx:xx:xx)
hyphen	Sets the delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx)
single-hyphen	Sets the delimiter to a single hyphen (for example, xxxxxx-xxxxxx)
none	Disables delimiter (for example, xxxxxxxxxxxx)

Defaults

The default delimiter is hyphen.

Examples

```
> config radius auth mac-delimiter hyphen
```

Related Commands

show radius auth statistics

config radius auth management

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

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

Syntax Description	config	Configuration settings.
	radius auth	Default RADIUS authentication server.
	management	Configure a RADIUS server for management users.
	index	RADIUS server index.
	{enable disable}	Enable or disable the server as a management user’s default RADIUS Server.

Defaults None.

Examples > config radius auth management 1 enable

Related Commands show radius acct statistics
 config radius acct network

config radius auth network

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

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

Syntax Description	config	Configuration settings.
	radius auth	Default RADIUS authentication server.
	network	Configure a default RADIUS server for network users.
	<i>index</i>	RADIUS server index.
	{ enable disable }	Enable or disable the server as a network user default RADIUS Server.

Defaults	None.

Examples	> config radius auth network 1 enable

Related Commands	show radius acct statistics config radius acct network

config radius auth retransmit-timeout

To change the 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	config	Configuration settings.
	radius auth	RADIUS authentication server.
	retransmit-timeout	Configure retransmission timeout.
	index	RADIUS server index.
	timeout	Number of seconds (from 2 to 30) between retransmissions.

Defaults None.

Examples > config radius auth retransmit-timeout 5

Related Commands show radius auth statistics

config radius auth rfc3576

To configure RADIUS rfc3576 support for the authentication server for the Cisco Wireless LAN controller, use the **config radius auth rfc3576** command.

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

Syntax Description	config	Configuration settings.
	radius auth	Default RADIUS authentication server.
	rfc3576	Configure RADIUS rfc3576 support.
	{enable disable}	Enable or disable RFC-3576 support for an authentication server.
	<i>index</i>	RADIUS server index.

Defaults None.

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

Examples > **config radius auth rfc3576 enable 2**

Related Commands

- show radius auth statistics
- show radius summary
- show radius rfc3576

config radius auth server-timeout

To configures the 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	config	Configuration settings.
	radius auth	Default RADIUS authentication server.
	server-timeout	Configure the retransmission timeout value for a RADIUS accounting server
	<i>index</i>	RADIUS server index.
	<i>timeout</i>	Timeout value, valid range is 2 to 30 seconds

Defaults Default timeout: 2 seconds.

Examples > config radius auth server-timeout 2 10

Related Commands show radius auth statistics
show radius summary

config radius aggressive-failover disabled

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

config radius aggressive-failover disabled

Syntax Description	This command does not have any arguments or keywords.

Defaults	None.

Examples	<pre>> config radius aggressive-failover disabled</pre>

Related Commands	show radius summary

config radius backward compatibility

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

config radius backward compatibility {enable | disable}

Syntax Description

config	Configuration settings.
radius backward	RADIUS authentication server.
compatibility	Configure RADIUS backward compatibility.
{enable disable}	Enable or disable RADIUS vendor ID backward compatibility.

Defaults

Enabled.

Examples

```
> config radius backward compatibility disable
```

Related Commands

show radius summary

config radius callStationIdType

To configure callStationIdType information sent in radius messages for the Cisco Wireless LAN controller, use the **config radius callStationIdType** command. This command uses the selected calling station ID for communications with RADIUS servers and other applications.

```
config radius callStationIdType {ipAddr | macAddr | ap-macAddr}
```

Syntax Description	config	Configuration settings.
	radius	Configure callStationIdType information.
	callStationIdType	
	ipAddr macAddr ap-macAddr	- Enter ipAddr to configure Call Station ID type to IP address (only layer 3). - Enter macAddr to configure Call Station ID type to the system's MAC address (layers 2 and 3). - Enter ap-macAddr to configure Call Station ID type to use the access point's MAC address (layers 2 and 3).

Defaults Enabled.

Examples

```
> config radius callStationIdType ipAddr
> config radius callStationIdType macAddr
> config radius callStationIdType ap-macAddr
```

Related Commands show radius summary

config rfid auto-timeout

To configure the automatic timeout of RFID tags, use the **config rfid auto-timeout** command.

```
config rfid auto-timeout {enable | disable}
```

Syntax Description	config	Configuration settings.
	rfid auto-timeout	Configure automatic timeout of RFID tags.
	{enable disable}	Enable or disable automatic timeout.

Defaults None.

Examples > config rfid auto-timeout enable

Related Commands

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

config rfid status

To configure RFID tag data collection, use the **config rfid status** command.

config rfid status {enable | disable}

Syntax Description	config	Configuration settings.
	rfid status	Configure RFID tag data collection.
	{enable disable}	Enable or disable RFID tag tracking.

Defaults	None.

Examples	> config rfid status enable

Related Commands	show rfid summary, config rfid auto-timeout config rfid timeout

config rfid timeout

To configure the static RFID tag data timeout, use the **config rfid timeout** command.

config rfid timeout *seconds*

Syntax Description	show	Display settings.
	rfid timeout	Configure the static RFID tag data timeout.
	<i>seconds</i>	Timeout in seconds (from 60 to 7200).

Defaults

None.

Examples

> **config rfid timeout 60**

Related Commands

show rfid summary
config rfid statistics

Configure Rogue Commands

Use the configure rogue commands to configure policy settings for unidentified (rogue) clients.

config rogue adhoc

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

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

Syntax Description	
config	Configuration settings.
rogue	Rogue access point settings.
adhoc	Ad-hoc rogue access point settings.
enable disable	Globally enable or disable detection and reporting of ad-hoc rogues.
external	Acknowledge the presence of the ad-hoc rogue.
<i>rogue_MAC</i>	MAC address of the ad-hoc rogue access point.
alert	Generate an SMNP trap upon detection of the ad-hoc rogue, and generate an immediate alert to the system administrator for further action.
all	Enable alerts for all ad-hoc rogue access points.
auto-contain	Enter auto-contain without the optional <i>monitor_ap</i> to automatically contain all wired ad-hoc rogues detected by the controller.
<i>monitor_ap</i>	(Optional) IP address of the ad-hoc rogue access point. Enter auto-contain with the <i>monitor_ap</i> argument to monitor the rogue access point without containing it.
contain	Contain the offending device so that its signals no longer interfere with authorized clients.
<i>1234_aps</i>	Maximum number of Cisco access points assigned to actively contain the ad-hoc rogue access point (1 through 4, inclusive).

Defaults

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

Usage Guidelines

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



Note

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

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

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

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

Examples

```
> config rogue adhoc enable
> config rogue adhoc alert all
> config rogue adhoc contain 11:11:11:11:11:11 3
```

Related Commands

[show rogue ignore-list](#)
[show rogue rule detailed](#)
[show rogue rule summary](#)

config rogue ap classify

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

```
config rogue ap classify {friendly state {internal | external} ap_mac
config rogue ap classify {malicious | unclassified} state {alert | contain} ap_mac
```

Syntax Description		
config		Configuration settings.
rogue		Unidentified network device settings.
ap		Rogue access point settings.
classify		Classify rogue access point.
friendly		Classify a rogue access point as friendly.
malicious		Classify a rogue access point as potentially malicious.
unclassified		Classify a rogue access point as unknown.
state		Response to classification.
internal		Configure controller to trust this rogue access point.
external		Configure controller to acknowledge the presence of this access point.
alert		Configure controller to forward an immediate alert to the system administrator for further action.
contain		Configure controller to contain the offending device so that its signals no longer interfere with authorized clients.
<i>ap_mac</i>		MAC address of the rogue access point.

Defaults

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

Usage Guidelines

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

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

Examples

To classify a rogue access point as friendly and can be trusted, enter this command:

```
> config rogue ap classify friendly state internal 11:11:11:11:11:11
```

To classify a rogue access point as malicious and to send an alert, enter this command:

```
> config rogue ap classify malicious state alert 11:11:11:11:11:11
```

To classify a rogue access point as unclassified and to contain it, enter this command:

```
> config rogue ap classify unclassified state contain 11:11:11:11:11:11
```

Related Commands

config rogue ap friendly
config rogue ap rldp
config rogue ap ssid
config rogue ap timeout
config rogue ap valid-client
config rogue rule
config trapflags rogueap
show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue ap friendly

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

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

Syntax Description	config	Configuration settings.
	rogue	Unidentified network device settings.
	ap	Rogue access point settings.
	friendly	Settings for rogue access points classified as friendly.
	add delete	Add or delete this rogue access point from the friendly MAC address list.
	<i>ap_mac</i>	MAC address of the rogue access point you want to add or delete.

Defaults None.

Examples To add a new friendly access point with MAC address 11:11:11:11:11:11 to the friendly MAC address list, enter this command:

```
> config rogue ap friendly add 11:11:11:11:11:11
```

Related Commands

- [config rogue ap classify](#)
- [config rogue ap rldp](#)
- [config rogue ap ssid](#)
- [config rogue ap timeout](#)
- [config rogue ap valid-client](#)
- [config rogue rule](#)
- [config trapflags rogueap](#)
- [show rogue ap clients](#)
- [show rogue ap detailed](#)
- [show rogue ap summary](#)
- [show rogue ap friendly summary](#)
- [show rogue ap malicious summary](#)
- [show rogue ap unclassified summary](#)
- [show rogue ignore-list](#)
- [show rogue rule detailed](#)
- [show rogue rule summary](#)

config rogue ap rldp

To enable, disable, or initiate Rogue Location Discovery Protocol (RLDP), enter these commands.

```
config rogue ap rldp enable {alarm-only | auto-contain} [monitor_ap_only]
config rogue ap rldp initiate rogue_mac_address
config rogue ap rldp disable
```

Syntax Description

config	Configuration settings.
rogue	Unidentified network device settings.
ap	Rogue access point settings.
rldp	Configure RLDP.
enable	Enable RLDP on all access points.
alarm-only	When entered without the optional argument <i>monitor_ap_only</i> , enables RLDP on all access points.
auto-contain	When entered without the optional argument <i>monitor_ap_only</i> , automatically contains all rogue access points.
<i>monitor_ap_only</i>	(Optional) Enable RLDP (when used with alarm-only keyword), or enable automatically containment (when used with auto-contain keyword) only on the designated monitor access point.
initiate	Initiate RLDP on a specific rogue access point.
<i>rogue_mac_address</i>	MAC address of specific rogue access point.
disable	Disable RLDP on all access points.

Defaults

None.

Usage Guidelines

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

Examples

To enable RLDP on all access points, enter this command:

```
> config rogue ap rldp enable alarm-only
```

To enable RLDP on monitor-mode access point *cisco_ap_1*, enter this command:

```
> config rogue ap rldp enable alarm-only cisco_ap_1
```

To start RLDP on the rogue access point with MAC address 123.456.789.000, enter this command:

```
> config rogue ap rldp initiate 123.456.789.000
```

To disable RLDP on all access points, enter this command:

```
> config rogue ap rldp disable
```


Related Commands

config rogue ap classify
config rogue ap friendly
config rogue ap ssid
config rogue ap timeout
config rogue ap valid-client
config rogue rule
config trapflags rogueap
show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue ap ssid

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

config rogue ap ssid {alarm | auto-contain}

Syntax Description

config	Configuration settings.
rogue	Unidentified network device settings.
ap	Rogue access point settings.
ssid	Policy settings for rogue access points that are advertising your network SSID.
alarm	Generate only an alarm when a rogue ap is discovered to be advertising your network's SSID.
auto-contain	Automatically contain the rogue access point that is advertising your network's SSID.

Defaults

None.

Usage Guidelines

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

Examples

To automatically contain a rogue access point that is advertising your network's SSID, enter this command:

```
> config rogue ap ssid auto-contain
```

Related Commands

[config rogue ap classify](#)
[config rogue ap friendly](#)
[config rogue ap rldp](#)
[config rogue ap timeout](#)
[config rogue ap valid-client](#)
[config rogue rule](#)
[show rogue ap clients](#)
[show rogue ap detailed](#)
[show rogue ap summary](#)
[show rogue ap friendly summary](#)
[show rogue ap malicious summary](#)
[show rogue ap unclassified summary](#)
[show rogue ignore-list](#)
[show rogue rule detailed](#)
[show rogue rule summary](#)

config rogue ap 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	config	Configuration settings.
	rogue	Unidentified network device settings.
	ap	Rogue access point settings.
	timeout	Rogue access point list expiration settings.
	<i>seconds</i>	A value of 240 to 3600 seconds (inclusive), with a default value of 1200 seconds.

Defaults 1200 seconds.

Examples To set an expiration time for entries in the rogue access point and client list to 2400 seconds, enter this command:
 > **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 ap valid-client](#)
- [config rogue rule](#)
- [config trapflags rogueap](#)
- [show rogue ap clients](#)
- [show rogue ap detailed](#)
- [show rogue ap summary](#)
- [show rogue ap friendly summary](#)
- [show rogue ap malicious summary](#)
- [show rogue ap unclassified summary](#)
- [show rogue ignore-list](#)
- [show rogue rule detailed](#)
- [show rogue rule summary](#)

config rogue ap valid-client

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

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

Syntax Description

config	Configuration settings.
rogue	Unidentified network device settings.
ap	Rogue access point settings.
valid-client	Settings for valid clients associated with rogue access points.
alarm	Generate only an alarm when a rogue ap is discovered to be associated with a valid client.
auto-contain	Automatically contain a rogue access point to which a trusted client is associated.

Defaults

None.

Usage Guidelines

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

Examples

To automatically contain a rogue access point that is associated with a valid client, enter this command:

```
> config rogue ap valid-client auto-contain
```

Related Commands

[config rogue ap classify](#)
[config rogue ap friendly](#)
[config rogue ap rldp](#)
[config rogue ap ssid](#)
[config rogue ap timeout](#)
[config rogue rule](#)
[config trapflags rogueap](#)
[show rogue ap clients](#)
[show rogue ap detailed](#)
[show rogue ap summary](#)
[show rogue ap friendly summary](#)
[show rogue ap malicious summary](#)
[show rogue ap unclassified summary](#)
[show rogue ignore-list](#)
[show rogue rule detailed](#)
[show rogue rule summary](#)

config rogue client

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

config rogue client {**aaa** {**enable** | **disable**} | **alert** *ap_mac* | **contain** *client_mac*} *num_of_APs*

Syntax Description	
config	Configuration settings.
rogue	Unidentified network device settings.
client	Client settings.
aaa	Configure AAA server or local database to validate whether rogue clients are valid clients.
enable disable	Enable or disable the AAA server or local database to check rogue client MAC addresses for validity.
aaa	Configure the AAA server or local database to validate whether or not rogue clients are valid clients.
alert	Configure controller to forward an immediate alert to the system administrator for further action.
contain	Configure controller to contain the offending device so that its signals no longer interfere with authorized clients.
enable disable	- Enter enable to enable the AAA server or local database to check MAC addresses of a rogue clients for validity. - Enter disable to disable the AAA server or local database from checking MAC addresses of rogue clients for validity.
<i>client_mac</i>	MAC address of the rogue client.
<i>num_of_APs</i>	The maximum number of Cisco access points to actively contain the rogue access point (1–4).

Defaults None.

Examples

```
> config rogue client aaa enable
> config rogue client aaa disable
> config rogue client alert 11:11:11:11:11:11
> config rogue client contain 11:11:11:11:11:11 2
```

Related Commands

- [config rogue rule](#)
- [config trapflags rogueap](#)
- [show rogue ap clients](#)
- [show rogue client detailed](#)
- [show rogue client summary](#)
- [show rogue ignore-list](#)
- [show rogue rule detailed](#)
- [show rogue rule summary](#)

config rogue detection

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

config rogue detection {enable | disable} {Cisco_AP | all}

Syntax Description

config	Configuration settings.
rogue	Unidentified network device settings.
detection	Detect rogue devices.
enable disable	Enable or disable rogue detection on this access point.
<i>Cisco_AP</i>	Cisco access point.
all	All access points.

Defaults

Enabled.

Usage Guidelines

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

Examples

```
> config rogue detection enable CISCO_AP
```

Related Commands

[config rogue rule](#)
[config trapflags rogueap](#)
[show rogue ap clients](#)
[show rogue client detailed](#)
[show rogue client summary](#)
[show rogue ignore-list](#)
[show rogue rule detailed](#)
[show rogue rule summary](#)

config rogue rule

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

```
config rogue rule {add ap priority priority classify {friendly | malicious} rule_name |
  classify {friendly | malicious} rule_name |
  condition ap {set | delete} condition_type condition_value rule_name |
  {enable | delete | disable} {all | rule_name} |
  match {all | any} |
  priority priority rule_name}
```

Syntax Description

config	Configuration settings.
rogue	Unidentified network device settings.
rule	Configure rogue rule.
add ap priority	Adds a rule with match any criteria and the priority you specify.
<i>priority</i>	Specify the priority of this rule within the list of rules.
classify	Specify the classification of a rule.
friendly malicious	- Enter friendly to classify a rule as friendly. - Enter malicious to classify a rule as malicious.
<i>rule_name</i>	The rule to which the command applies, or the name of a new rule.
condition ap	Specify the conditions for a rule that the rogue access point must meet.
set delete	- Enter set to add conditions to a rule that the rogue access point must meet. - Enter delete to remove conditions to a rule that the rogue access point must meet.
<i>condition_type</i>	The type of the condition to be configured. The condition types are listed below: client-count—Requires that a minimum number of clients be associated to the rogue access point. Valid range is 1 to 10 (inclusive) duration—Requires that the rogue access point be detected for a minimum period of time. Valid range is 0 to 3600 seconds (inclusive) managed-ssid—Requires that the rogue access point's SSID be known to the controller. no-encryption—Requires that the rogue access point's advertised WLAN does not have encryption enabled. rssi—Requires that the rogue access point have a minimum RSSI value. Valid range is -95 to -50 dBm (inclusive) ssid—Requires that the rogue access point have a specific SSID.
<i>condition_value</i>	The value of the condition. This value is dependent upon condition_type. For instance, if the condition type is ssid , then the condition value is either the SSID name, or all .

enable delete disable	• Enter enable to enable all rules or a single specific rule. • Enter delete to delete all rules or a single specific rule. • Enter disable to disable all rules or a single specific rule.
match	Specify whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.
all any	• Enter all to effect all rules defined. • Enter any to effect any rule meeting certain criteria.
priority	Enter priority to change the priority of a specific rule and shift others in the list accordingly.

Defaults

None.

Usage Guidelines

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

ExamplesTo create a rule called **rule_1** with a priority of **1** and a classification as **friendly**, enter this command:

```
> config rogue rule add ap priority 1 classify friendly rule_1
```

To enable rule_1, enter this command:

```
> config rogue rule enable rule_1
```

To change the priority of the last command, enter this command:

```
> config rogue rule priority 2 rule_1
```

To change the classification of the last command, enter this command:

```
> config rogue rule classify malicious rule_1
```

To disable the last command, enter this command:

```
> config rogue rule disable rule_1
```

To delete SSID_2 from the user-configured SSID list in rule-5, enter this command:

```
> config rogue rule condition ap delete ssid ssid_2 rule-5
```

Related Commands

[config rogue adhoc](#)
[config rogue ap classify](#)
[config rogue ap friendly](#)
[config rogue ap rldp](#)
[config rogue ap ssid](#)
[config rogue ap timeout](#)
[config rogue ap valid-client](#)
[config rogue client](#)
[config trapflags rogueap](#)
[show rogue ap clients](#)
[show rogue ap detailed](#)

show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue client detailed
show rogue client summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config route add

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

config route add *ip_address netmask gateway*

Syntax Description

config	Configuration settings.
route	Network route.
add	Add a route.
<i>ip_address</i>	Network IP Address.
<i>netmask</i>	The subnet mask for the network.
<i>gateway</i>	IP Address of the gateway for the route network.

Defaults

None.

Examples

```
> config route add 10.1.1.0 255.255.255.0 10.1.1.1
```

Related Commands

show route summary
config route delete

config route delete

To remove a network route from the Service Port, use the **config route delete** command.

config route delete *ip_address*

Syntax Description	config	Configuration settings.
	route	Network route.
	delete	Delete a route.
	<i>ip_address</i>	Network IP Address.

Defaults None.

Examples > **config route delete 10.1.1.0**

Related Commands show route all, config route add

config serial baudrate

To set the serial port baud rate, use the **config serial baudrate** command.

```
config serial baudrate { 1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 }
```

Syntax Description	config	Configuration settings.
	serial baudrate	Configure serial port baud rate.
	1200 2400 4800 9600 19200 38400 57600	Enter one of the supported connection speeds.

Defaults	9600.

Examples	> config serial baudrate 9600

Related Commands	config serial timeout

config serial timeout

To set the timeout of a serial port session, use the **config serial timeout** command.

Use this command to set the timeout for a serial connection to the front of the Cisco Wireless LAN controller from 0 to 160 minutes where 0 is no timeout.

config serial timeout *minutes*

Syntax Description	config	Configuration settings.
	serial	Serial connection settings.
	timeout	Configure timeout of a serial port session.
	<i>minutes</i>	Timeout in minutes from 0 to 160. A value of 0 indicates no timeout.

Defaults	0 (no timeout).

Examples	> config serial timeout 10

Related Commands	config serial timeout

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

config	Configuration settings.
service	Configure service settings.
timestamps	Configure timestamps.
debug	Configure timestamps in debug messages.
log	Configure timestamps in log messages.
datetime disable	- Enter datetime to timestamp message logs with the standard date and time. - Enter disable to prevent message logs being timestamped.

Defaults

Disabled.

Examples

```
> config service timestamps log datetime
> 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. Up to five sessions are possible while a setting of zero prohibits any telnet CLI sessions.

config sessions maxsessions *session_num*

Syntax Description	config	Configuration settings.
	sessions	Telnet CLI session settings.
	maxsessions	Configure the number of allowed CLI sessions.
	<i>session_num</i>	Number of sessions from 0 to 5.

Defaults	5.

Examples	> 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	config	Configuration settings.
	sessions	Telnet CLI session settings.
	timeout	Configure the inactivity timeout for telnet CLI sessions
	<i>timeout</i>	Timeout of telnet session in minutes (from 0 to 160). A value of 0 indicates no timeout.

Defaults	5.

Examples	> config sessions timeout 20

Related Commands	show sessions

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	
config	Configuration settings.
snmp	SNMP settings.
community	SNMP community settings.
accessmode	Configure the access mode for an SNMP community.
ro rw	- Enter ro to specify a Read Only mode. - Enter rw to specify a Read/Write mode.
name	SNMP community name.

Defaults

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

```
> 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. Use this command to create a new community with the following default configuration:

config snmp community create *name*

Syntax Description

config	Configuration settings.
snmp	SNMP settings.
community	SNMP community settings.
create	Create a new community.
<i>name</i>	SNMP community name. Up to 16 characters.

Defaults

None.

Examples

```
> config snmp community create test
```

```
> 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
test	0.0.0.0	0.0.0.0	Read Only	Disable

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	config	Configuration settings.
	snmp	SNMP settings.
	community	SNMP community settings.
	delete	Delete an SNMP community.
	<i>name</i>	SNMP community name.

Defaults	None.

Examples	<pre>> config snmp community delete test</pre>

Related Commands	<pre>show snmp community config snmp community mode config snmp community accessmode config snmp community create config snmp community ipaddr</pre>

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

config	Configuration settings.
snmp	SNMP settings.
community	SNMP community settings.
ipaddr	Set IP Address settings.
ip_address	SNMP community IP address.
ip_mask	SNMP community subnet mask.
name	SNMP community name.

Defaults

None.

Examples

```
> config snmp community ipaddr 10.10.10.10.2 255.255.255.0 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 ipaddr

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	config snmp community	Configure SNMP community settings.
	mode	Configure an SNMP community
	enable disable	Enable or disable the community.
	<i>name</i>	SNMP community name.

Defaults None.

Examples

```
> config snmp community mode disable public
```

Related Commands

```
show snmp community
config snmp community accessmode
config snmp community create
config snmp community delete
config snmp community ipaddr
```

config snmp syscontact

To set the SNMP system contact name, use the **config snmp syscontact** command.

config snmp syscontact *contact*

Syntax Description

config	Configuration settings.
snmp	SNMP settings.
syscontact	Set the SNMP system contact name.
<i>contact</i>	SNMP system contact name. Up to 31 alphanumeric characters.

Defaults

None.

Examples

```
> 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	config	Configuration settings.
	snmp	SNMP settings.
	syslocation	configure the SNMP system location name.
	<i>location</i>	SNMP system location name. Up to 31 alphanumeric characters.

Defaults	None.

Examples	> config snmp syslocation Building_2a

Related Commands	show snmpcommunity

config snmp trapreceiver create

To add server to receive a SNMP traps, use the **config snmp trapreceiver create** command. The IP address must be valid for the command to add the new server.

config snmp trapreceiver create *name ip_address*

Syntax Description

config	Configuration settings.
snmp	SNMP settings.
trapreceiver	SNMP trap server settings.
create	Add a new SNMP trap receiver.
<i>name</i>	SNMP community name. Up to 16 characters.
<i>ip_address</i>	SNMP community IP address.

Defaults

None.

Examples

```
> 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	config	Configuration settings.
	snmp	SNMP settings.
	trapreceiver	Server to receive traps.
	delete	Delete an SNMP trap receiver.
	<i>name</i>	SNMP community name. Up to 16 characters.

Defaults	None.

Examples	> 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. This enables or disables the Cisco Wireless LAN controller from sending the traps to the selected server.

config snmp trapreceiver mode {enable | disable} name

Syntax Description	config	Configuration settings.
	snmp	SNMP settings.
	trapreceiver	Server to receive traps.
	mode	Configure an SNMP trap receiver.
	{enable disable}	Enable or disable an SNMP trap receiver.
	<i>name</i>	SNMP community name.

Defaults None.

Examples > 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
config	Configuration settings.
snmp	SNMP settings.
v3user create	Creates a version 3 SNMP user.
<i>username</i>	Version 3 SNMP username.
{ro rw}	- Enter ro to specify a read-only user privilege. - Enter rw to specify a read-write user privilege.
{none hmacmd5 hmacsha}	- Enter none if no authentication is required. - Enter hmacmd5 to use Hashed Message Authentication Coding-Message Digest 5 (HMAC-MD5) for authentication. - Enter hmacsha to use Hashed Message Authentication Coding-Secure Hashing Algorithm (HMAC-SHA) for authentication.
{none des aes}	- Enter none if no encryption is required. - Enter des to use Cipher Block Chaining-Digital Encryption Standard (CBC-DES) encryption. - Enter aescfb128 to use Cipher Feedback Mode-Advanced Encryption Standard-128 (CFB-AES-128) encryption.
[<i>auth_key</i>]	Authentication key for the HMAC-MD5 or HMAC-SHA authentication protocol.
[<i>encrypt_key</i>]	Encryption key for the CBC-DES or CFB-AES-128 encryption protocol.

Defaults	SNMP v3 User Name	AccessMode	Authentication	Encryption
default		Read/Write	HMAC-SHA	CFB-AES

Examples	To add an SNMP username called “test” with read-only privileges and no encryption or authentication, enter this command:

```
> config snmp v3user create test ro none none
```

Related Commands

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

config	Configuration settings.
snmp	SNMP settings.
v3user	Version 3 SNMP.
delete	Delete a v3 user.
<i>username</i>	Username to delete.

Defaults

None.

Examples

This will 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	config	Configuration settings.
	snmp	SNMP settings.
	version	Configure SNMP version.
	{v1 v2 v3}	Enter an SNMP version to enable or disable.
	{enable disable}	Enable or disable specified version

Defaults	All versions enabled

Examples	> config sessions timeout 20

Related Commands	show snmpversion

Configure Spanning Tree Protocol Commands

Use the **config spanningtree** commands to configure SpanningTree protocol settings.

config spanningtree port mode

To turn fast or 802.1D Spanning Tree Protocol on or off for one or all Cisco Wireless LAN controller ports, use the **config spanningtree port mode** command.

config spanningtree port mode {off | 802.1d | fast} {port | all}

Syntax Description

config	Configuration settings.
spanningtree	Spanning Tree Protocol.
port	Configure spanning tree values on a per port basis.
mode	Configure the STP port mode.
{off 802.1d fast}	Enter a supported port mode or off to disable STP for the specified ports.
{port all}	Enter a port number (1 through 12 or 1 through 24), or all to configure all ports.

Defaults

Port STP = off.

Usage Guidelines

When the a Cisco 4400 series wireless LAN controller is configured for port redundancy, Spanning Tree Protocol must be disabled for all ports on the Cisco 4400 series wireless LAN controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 series wireless LAN controller.

Note that you must disable Cisco Wireless LAN controller STP using the config spanningtree switch mode command, select STP mode for all Ethernet ports using this command, and then enable Cisco Wireless LAN controller STP using the config spanningtree switch mode command. This procedure allows the Cisco Wireless LAN controller to most efficiently set up STP, detect logical network loops, place redundant ports on standby, and build a network with the most efficient pathways.

Examples

To disable STP for all Ethernet ports:

```
> config spanningtree port mode off all
```

To turn on STP 802.1D mode for Ethernet port 24:

```
> config spanningtree port mode 802.1d 24
```

To turn on fast STP mode for Ethernet port 2:

```
> config spanningtree port mode fast 2
```

Related Commands

show spanningtree port
config spanningtree switch mode
config spanningtree port pathcost
config spanningtree port priority

config spanningtree port pathcost

To set the STP path cost for an Ethernet port, use the **config spanningtree port pathcost** command.

config spanningtree port pathcost {*cost* | **auto**} {*port* | **all**}

Syntax Description	config	Configuration settings.
	spanningtree	Spanning Tree Protocol.
	port	Configure spanning tree values on a per port basis.
	pathcost	Configure the STP port path cost.
	{ <i>cost</i> auto }	Enter cost in decimal as determined by the network planner or auto (default cost).
	{ <i>port</i> all }	Enter a port number (1 through 12 or 1 through 24), or all to configure all ports.

Defaults auto.

Usage Guidelines When the a Cisco 4400 series wireless LAN controller is configured for port redundancy, Spanning Tree Protocol must be disabled for all ports on the Cisco 4400 series wireless LAN controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 series wireless LAN controller.

Examples To have the STP algorithm automatically assign a path cost for all ports:

```
> config spanningtree port pathcost auto all
```

To have the STP algorithm use a port cost of 200 for port 22:

```
> config spanningtree port pathcost 200 22
```

Related Commands

- show spanningtree port
- config spanningtree port mode
- config spanningtree port priority

config spanningtree port priority

To configure the STP port priority, use the **config spanningtree port priority** command.

config spanningtree port priority *priority_num port*

Syntax Description

config	Configuration settings.
spanningtree	Spanning Tree Protocol.
port	Configure spanning tree values on a per port basis.
priority	Configure the STP port priority.
<i>priority_num</i>	Enter a priority number from 0 to 255.
<i>port</i>	Enter a port number (1 through 12 or 1 through 24).

Defaults

STP Priority = 128.

Usage Guidelines

When the a Cisco 4400 series wireless LAN controller is configured for port redundancy, Spanning Tree Protocol must be disabled for all ports on the Cisco 4400 series wireless LAN controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 series wireless LAN controller.

Examples

To set Ethernet port 2 to STP priority 100:

```
> config spanningtree port priority 100 2
```

Related Commands

show spanningtree port
config spanningtree switch mode
config spanningtree port mode
config spanningtree port pathcost

config spanningtree switch bridgepriority

To set the bridge ID, use the **config spanningtree switch bridgepriority** command.

config spanningtree switch bridgepriority *priority_num*

Syntax Description	config	Configuration settings.
	spanningtree	Spanning Tree Protocol.
	switch	Configure spanning tree values on a per switch basis.
	bridgepriority	Configure the STP bridge priority.
	priority_num	Enter a priority number between 0 and 65535.

Defaults The factory default is 32768.



Usage Guidelines **Note** When the a Cisco 4400 series wireless LAN controller is configured for port redundancy, Spanning Tree Protocol must be disabled for all ports on the Cisco 4400 series wireless LAN controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 series wireless LAN controller.

The value of the writable portion of the Bridge ID, that is, the first two octets of the (8 octet long) Bridge ID. The other (last) 6 octets of the Bridge ID are given by the value of Bridge MAC Address. The value may be specified as a number between 0 and 65535.

Examples

```
> config spanningtree switch bridgepriority 40230
```

Related Commands

- show spanningtree switch
- config spanningtree switch forwarddelay
- config spanningtree switch hellotime
- config spanningtree switch maxage
- config spanningtree switch mode

config spanningtree switch forwarddelay

To set the bridge timeout, use the **config spanningtree switch forwarddelay** command.

config spanningtree switch forwarddelay *seconds*

Syntax Description	config	Configuration settings.
	spanningtree	Spanning Tree Protocol.
	switch	Configure spanning tree values on a per switch basis.
	forwarddelay	Configure the STP bridge forward delay.
	<i>seconds</i>	Timeout in seconds (between 4 and 30).

Defaults The factory default is 15.

Usage Guidelines The value that all bridges use for **forwarddelay** when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this setting is related to the value of STP Bridge Maximum Age. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent may return a badValue error if a set is attempted to a value which is not a whole number of seconds. The Factory default is 15. Valid values are 4 through 30 seconds.

Examples > **config spanningtree switch forwarddelay 20**

Related Commands

- [config spanningtree switch bridgepriority](#)
- [config spanningtree switch hellotime](#)
- [config spanningtree switch maxage](#)
- [config spanningtree switch mode](#)
- [config switchconfig flowcontrol](#)

config spanningtree switch hellotime

To set the hello time, use the **config spanningtree switch hellotime** command.

config spanningtree switch hellotime *seconds*

Syntax Description	config	Configuration settings.
	spanningtree	Spanning Tree Protocol.
	switch	Configure spanning tree values on a per switch basis.
	hellotime	Configure the STP hello time.
	<i>seconds</i>	STP hello time in seconds.

Defaults The factory default is 15.

Usage Guidelines This is the value all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D- 1990 to be 1 second. Valid values are 1 through 10 seconds.

Examples
> **config spanningtree switch hellotime 4**

Related Commands
show spanningtree switch
spanningtree switch bridgepriority
config spanningtree switch forwarddelay
config spanningtree switch maxage
config spanningtree switch mode

config spanningtree switch maxage

To set the maximum age, use the **config spanningtree switch maxage** command.

config spanningtree switch maxage *seconds*

Syntax Description	config	Configuration settings.
	spanningtree	Spanning Tree Protocol.
	switch	Configure spanning tree values on a per switch basis.
	maxage	Configure the STP bridge maximum age.
	<i>seconds</i>	STP bridge maximum age in seconds.

Defaults The factory default is 20.

Usage Guidelines This is the value all bridges use for MaxAge when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Hello Time. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 6 through 40 seconds.

Examples > **config spanningtree switch maxage 30**

Related Commands

- show spanningtree switch
- config spanningtree switch bridgepriority
- config spanningtree switch forwarddelay
- config spanningtree switch hellotime
- config spanningtree switch mode

config spanningtree switch mode

To turn the Cisco Wireless LAN controller Spanning Tree Protocol on or off, use the **config spanningtree switch mode** command.

config spanningtree switch mode {enable | disable}

Syntax Description	config	Configuration settings.
	spanningtree	Spanning Tree Protocol.
	switch	Configure spanning tree values on a per switch basis.
	mode	Configure Spanning Tree Protocol on the switch.
	{enable disable}	Enable or disable Spanning Tree Protocol on the switch.

Defaults STP = Disabled.

Usage Guidelines Note that you must disable the Cisco Wireless LAN controller STP using this command, select STP mode for all Ethernet ports using the config spanningtree port mode command, and then enable the Cisco Wireless LAN controller STP using this command. This procedure allows the Cisco Wireless LAN controller to most efficiently set up STP, detect logical network loops, place redundant ports on standby, and build a network with the most efficient pathways.

Examples To support STP on all Cisco Wireless LAN controller Ports:

```
> config spanningtree switch mode enable
```

Related Commands

- show spanningtree switch
- config spanningtree switch bridgepriority
- config spanningtree switch forwarddelay
- config spanningtree switch hellotime
- config spanningtree switch maxage
- config spanningtree port mode

config switchconfig flowcontrol

To enable or disable 802.3x flow control, use the **config switchconfig flowcontrol** command.

```
config switchconfig flowcontrol {enable | disable}
```

Syntax Description	config	Configuration settings.
	switchconfig	Cisco Wireless LAN controller parameters.
	flowcontrol	Configure flow control.
	{enable disable}	Enable or disable 802.3x flow control.

Defaults	Disabled

Examples	> config switchconfig flowcontrol enable

Related Commands	show switchconfig

config switchconfig mode

To configure LWAPP transport mode for Layer 2 or Layer 3, use the **config switchconfig flowcontrol** command.

config switchconfig mode {L2 | L3}

Syntax Description	config	Configuration settings.
	switchconfig	Cisco Wireless LAN controller parameters.
	mode	Configure LWAPP transport mode to Layer 2 or Layer 3.
	{L2 L3}	Enter a transport mode: L2 for Layer 2 or L3 for Layer 3.

Defaults	L3

Examples	> 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	config	Configuration settings.
	switchconfig	Cisco Wireless LAN controller parameters.
	{enable disable}	Enable or disable secret obfuscation.

Defaults 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 > 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	config	Configuration settings.
	sysname	Configures the system name.
	<i>name</i>	System name. Up to 31 alphanumeric characters.

Defaults	None.

Examples	> config sysname Ent_01

Related Commands	show sysinfo

Configure TACACS Commands

Use the **config tacacs** commands to configure TACACS+ settings.

config tacacs

To configure TACACS+ accounting, authentication, and authorization servers, use the **config tacacs** command.

config tacacs [acct | auth | athr]

Syntax Description	acct	(Optional) Configures a TACACS+ accounting server.
	auth	(Optional) Configures a TACACS+ authentication server
	athr	(Optional) Configures a TACACS+ authorization server

Defaults	None.

Examples	None.

Related Commands	show run-config show tacacs summary

config tacacs acct

To configure TACACS+ accounting server settings, use the **config tacacs acct** command.

```
config tacacs acct {add server_index ip_address port type secret_key |
  delete server_index |
  disable server_index |
  enable server_index |
  retransmit-timeout server_index seconds }
```

Syntax Description	
add	(Optional) Add a new TACACS+ accounting server.
<i>server_index</i>	Specifies the TACACS+ accounting server index (1 to 3).
<i>ip_address</i>	Specifies the IP address for the TACACS+ accounting server.
<i>port</i>	Specifies the controller port used for the TACACS+ accounting server.
<i>type</i>	Specifies the type of secret key being used (ASCII or HEX).
<i>secret_key</i>	Specifies the secret key in ASCII or hexadecimal characters.
delete	(Optional) Deletes a TACACS+ server.
disable	(Optional) Disables a TACACS+ server.
enable	(Optional) Enables a TACACS+ server.
retransmit-timeout	(Optional) Changes the default retransmit timeout for the TACACS+ server.
seconds	Specifies the retransmit timeout (2 to 30 seconds).

Defaults None.

Examples

```
> config tacacs acct add 1 10.0.0.0 10 ascii 12345678
> config tacacs acct retransmit-timeout 30
> config tacacs acct enable 1
```

Related Commands

```
show run-config
show tacacs acct statistics
show tacacs summary
```

config tacacs athr

To configure TACACS+ authorization server settings, use the **config tacacs athr** command.

```
config tacacs athr {add server_index ip_address port type secret_key |
    delete server_index |
    disable server_index |
    enable server_index |
    retransmit-timeout server_index seconds }
```

Syntax Description

add	(Optional) Add a new TACACS+ authorization server.
<i>server_index</i>	Specifies the TACACS+ authorization server index (1 to 3).
<i>ip_address</i>	Specifies the IP address for the TACACS+ authorization server.
<i>port</i>	Specifies the controller port used for the TACACS+ authorization server.
<i>type</i>	Specifies the type of secret key being used (ASCII or HEX).
<i>secret_key</i>	Specifies the secret key in ASCII or hexadecimal characters.
delete	(Optional) Deletes a TACACS+ server.
disable	(Optional) Disables a TACACS+ server.
enable	(Optional) Enables a TACACS+ server.
retransmit-timeout	(Optional) Changes the default retransmit timeout for the TACACS+ server.
seconds	Specifies the retransmit timeout (2 to 30 seconds).

Defaults

None.

Examples

```
> config tacacs athr add 3 10.0.0.0 4 ascii 12345678
> config tacacs athr retransmit-timeout 30
> config tacacs athr enable 3
```

Related Commands

```
show run-config
show tacacs athr statistics
show tacacs summary
```

config tacacs auth

To configure TACACS+ authentication server settings, use the **config tacacs auth** command.

```
config tacacs auth {add server_index ip_address port type secret_key |
  delete server_index |
  disable server_index |
  enable server_index |
  retransmit-timeout server_index seconds }
```

Syntax Description	
add	(Optional) Add a new TACACS+ authentication server.
<i>server_index</i>	Specifies the TACACS+ authentication server index (1 to 3).
<i>ip_address</i>	Specifies the IP address for the TACACS+ authentication server.
<i>port</i>	Specifies the controller port used for the TACACS+ authentication server.
<i>type</i>	Specifies the type of secret key being used (ASCII or HEX).
<i>secret_key</i>	Specifies the secret key in ASCII or hexadecimal characters.
delete	(Optional) Deletes a TACACS+ server.
disable	(Optional) Disables a TACACS+ server.
enable	(Optional) Enables a TACACS+ server.
retransmit-timeout	(Optional) Changes the default retransmit timeout for the TACACS+ server.
seconds	Specifies the retransmit timeout (2 to 30 seconds).

Defaults None.

Examples

```
> config tacacs auth add 2 10.0.0.3 6 ascii 12345678
> config tacacs auth retransmit-timeout 30
> config tacacs auth enable 2
```

Related Commands

```
show run-config
show tacacs auth statistics
show tacacs summary
```

config tacacs all

To configure a single TACACS+ server for accounting, authentication, and authorization, use the **config tacacs all** command.

```
config tacacs all (index ) (ip_address) (port) (secret_key)
```

Syntax Description	<i>index</i>	Specifies the TACACS+ server index (1 to 3).
	<i>ip_address</i>	Specifies the IP address of the TACACS+ server.
	<i>port</i>	Specifies the port used on the TACACS+ server.
	<i>secret_key</i>	Specifies the secret key in ASCII or hexadecimal characters.

Defaults None.

Examples None.

Related Commands show run-config
 show tacacs summary

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		
config		Command action.
time		Configures system time or servers.
manual		Configures the system time.
<i>MM/DD/YY</i>		Enter date.
<i>HH:MM:SS</i>		Enter time.

Defaults	None.

Examples	> config time manual 02/11/2003 15:29:00

Related Commands	show time

config time ntp

To set the Network Time Protocol, use the **config time ntp** command.

config time ntp {*interval seconds* | *server index ip_address*}

Syntax Description

config	Command action.
time	Configures system time or servers.
ntp	Configures the Network Time Protocol.
interval	
{interval server}	• Enter interval to configure the Network Time Protocol polling interval. • Enter server to configure the Network Time Protocol servers.
<i>seconds</i>	NTP polling interval in seconds (between 6800 and 604800).
<i>index</i>	NTP server index.
<i>ip_address</i>	NTP server's IP address. Use 0.0.0.0 to delete entry.

Defaults

None.

Examples

```
> config time ntp interval 7000
```

Related Commands

show time

config time timezone

To configure the system's timezone, use the **config time timezone** command.

config time timezone {enable | disable} *delta_hours delta_mins*

Syntax Description	config	Command action.
	time	Configures system time or servers.
	timezone	Disables or enables daylight savings time for the system.
	{enable disable}	Enable or disable daylight savings time.
	<i>delta_hours</i>	Enter the local hour difference from Universal Coordinated Time (UCT).
	<i>delta_mins</i>	Enter the local minute difference from UCT.

Defaults	None.

Examples	> config time timezone enable 2 0

Related Commands	show time

config time timezone location

To set the time zone location in order to have Daylight Savings Time (DST) set automatically when it occurs, use the **config time timezone location** command.

config time timezone location *location_index*

Syntax Description

config	Command action.
time	Configures system time or servers.
timezone	Enables daylight savings time for the system.
location	Configure the location automatically
<i>location_index</i>	A number representing the timezone required. The Timezones are as follows: 1. (GMT-12:00) International Date Line West 2. (GMT-11:00) Samoa 3. (GMT-10:00) Hawaii 4. (GMT-9:00) Alaska 5. (GMT-8:00) Pacific Time (US and Canada) 6. (GMT-7:00) Mountain Time (US and Canada) 7. (GMT-6:00) Central Time (US and Canada) 8. (GMT-5:00) Eastern Time (US and Canada) 9. (GMT-4:00) Atlantic Time (Canada) 10. (GMT-3:00) Buenos Aires (Argentina) 11. (GMT-2:00) Mid-Atlantic 12. (GMT-1:00) Azores 13. (GMT) London, Lisbon, Dublin, Edinburgh (default value) 14. (GMT +1:00) Amsterdam, Berlin, Rome, Vienna 15. (GMT +2:00) Jerusalem 16. (GMT +3:00) Baghdad 17. (GMT +4:00) Muscat, Abu Dhabi 18. (GMT +4:30) Kabul 19. (GMT +5:00) Karachi, Islamabad, Tashkent 20. (GMT +5:30) Colombo, Kolkata, Mumbai, New Delhi 21. (GMT +5:45) Katmandu 22. (GMT +6:00) Almaty, Novosibirsk 23. (GMT +6:30) Rangoon 24. (GMT +7:00) Saigon, Hanoi, Bangkok, Jakarta 25. (GMT +8:00) Hong Kong, Beijing, Chongqing 26. (GMT +9:00) Tokyo, Osaka, Sapporo 27. (GMT +9:30) Darwin 28. (GMT+10:00) Sydney, Melbourne, Canberra 29. (GMT+11:00) Magadan, Solomon Is., New Caledonia 30. (GMT+12:00) Kamchatka, Marshall Is., Fiji

Defaults

None.

Examples

```
> config time timezone location 10
```

Related Commands

```
show time
```

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-Security wepDecryptError {enable | disable}
```

Syntax Description	config	Configuration settings.
	trapflags	Trap settings.
	802.11-Security	802.11 security traps flag.
	wepDecryptError	Send the WEP decrypt error to clients.
	{enable disable}	Enable or disable sending 802.11 Security related traps.

Defaults	Enabled

Examples	> 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	config	Configuration settings.
	trapflags	Trap settings.
	aaa	Configure the of sending AAA related traps.
	{auth servers}	- Enter auth to enable trap sending when AAA authentication failure occurs for mgmt user or net user or macfilter. - Enter servers to enable trap sending when No Radius servers are responding.
	{enable disable}	Enable or disable the sending of AAA server related traps.

Defaults Enabled

Examples > **config trapflags aaa auth disable**

Related Commands **show trapflags**

config trapflags ap

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

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

Syntax Description

config	Configuration settings.
trapflags	Trap settings.
ap	Cisco lightweight access point traps flag.
{register interfaceUp}	- Enter register to enable sending trap when a Cisco lightweight access point registers with Cisco switch. - Enter interfaceUp to enable sending trap when a Cisco lightweight access point interface (A or B) comes up.
{enable disable}	Enable or disable sending access point related traps.

Defaults

Enabled

Examples

```
> config trapflags ap register disable
```

Related Commands

show trapflags

config trapflags authentication

To enable or disable sending traps on invalid SNMP access, use the **config trapflags authentication** command.

config trapflags authentication {enable | disable}

Syntax Description	config	Configuration settings.
	trapflags	Trap settings.
	authentication	Configure trap sending on invalid SNMP access.
	{enable disable}	Enable or disable sending traps on invalid SNMP access.

Defaults	Enabled

Examples	> 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-disassociate | 802.11-deauthenticate | 802.11-authfail |
                        802.11-assocfail | excluded } { enable | disable }
```

Syntax Description	config	Configuration settings.
	trapflags	Trap settings.
	client	Configure the sending of client related Dot11 traps.
	{802.11-disassociate 802.11-deauthenticate 802.11-authfail 802.11-assocfail excluded}	- Enter 802.11-disassociate to enable the sending of Dot11 disassociation traps to clients. - Enter 802.11-deauthenticate to enable the sending of Dot11 deauthentication traps to clients. - Enter 802.11-authfail to enable the sending of Dot11 authentication fail traps to clients. - Enter 802.11-assocfail to enable the sending of Dot11 association fail traps to clients. - Enter excluded to enable the sending of excluded trap to clients.
	{enable disable}	Enable or disable the sending of client related DOT11 traps.

Defaults Disabled

Examples > config trapflags client 802.11-disassociate disable

Related Commands show trapflags

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	config	Configuration settings.
	trapflags	Trap settings.
	configsave	Configure the sending of configuration saved traps.
	{enable disable}	Enable or disable the sending of configuration saved traps.

Defaults	Enabled

Examples	> config trapflags configsave disable

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	config	Configuration settings.
	trapflags	Trap settings.
	ipsec	IPSec trap flags.
	{esp-auth esp-reply invalidSPI ike-neg suite-neg invalid-cookie}	• Enable the sending of IPSec traps when ESP authentication failure occurs. • Enable the sending of IPSec traps when ESP replay failure occurs. • Enable the sending of IPSec traps when ESP invalid SPI is detected. • Enable the sending of IPSec traps when IKE negotiation failure occurs. • Enable the sending of IPSec traps when suite negotiation failure occurs. • Enable the sending of IPSec traps when Isakamp invalid cookie is detected.
	{enable disable}	Enable or disable the sending of IPSec traps.

Defaults Enabled

Examples > config trapflags ipsec esp-auth disable

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	config	Configuration settings.
	trapflags	Trap settings.
	linkmode	Configure switch-level link up/down trap flag.
	{enable disable}	Enable or disable Cisco Wireless LAN controller level Link up/down trap flags.

Defaults	Enabled

Examples	> config trapflags linkmode disable

Related Commands	show trapflags

config trapflags multiusers

To enable or disable the sending of traps when multiple logins active, use the **config trapflags multiusers** command.

```
config trapflags multiusers {enable | disable}
```

Syntax Description	config	Configuration settings.
	trapflags	Trap settings.
	multiusers	Configure trap sending when multiple logins are active.
	{enable disable}	Enable or disable the sending of traps when multiple logins active.

Defaults Enabled

Examples > config trapflags multiusers disable

Related Commands show trapflags

config trapflags rogueap

To enable or disable sending rogue access point detection traps, use the **config trapflags rogueap** command.

config trapflags rogueap {enable | disable}

Syntax Description

config	Configuration settings.
trapflags	Trap settings.
rogueap	Configure rogue access point detection trap sending.
enable disable	Enable or disable the sending of rogue access point detection traps.

Defaults

Enabled

Examples

```
> 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 RRM profile related traps, use the **config trapflags rrm-params** command.

```
config trapflags rrm-params {tx-power | channel | antenna} {enable | disable}
```

Syntax Description	config	Configuration settings.
	trapflags	Trap settings.
	rrm-params	RRM parameters traps flag.
	{tx-power channel antenna}	- Enter tx-power to enable trap sending when RF manager automatically changes tx-power level for the Cisco lightweight access point interface. - Enter channel to enable trap sending when RF manager automatically changes channel for the Cisco lightweight access point interface. - Enter antenna to enable trap sending when RF manager automatically changes antenna for the Cisco lightweight access point interface.
	{enable disable}	Enable or disable the sending of RRM profile related traps.

Defaults Enabled

Examples > config trapflags rrm-params tx-power disable

Related Commands show trapflags

config trapflags rrm-profile

To enable or disable the sending of RRM profile related traps, use the **config trapflags rrm-profile** command.

config trapflags rrm-profile {load | noise | interference | coverage} {enable | disable}

Syntax Description	
config	Configuration settings.
trapflags	Trap settings.
rrm-profile	RRM profile traps flag.
{load noise interference coverage}	- Enter load to enable trap sending when the load profile maintained by the RF manager fails. - Enter noise to enable trap sending when the noise profile maintained by the RF manager fails. - Enter interference to enable trap sending when the interference profile maintained by the RF manager fails. - Enter coverage to enable trap sending when the coverage profile maintained by the RF manager fails.
{enable disable}	Enable or disable the sending of RRM profile related traps.

Defaults Enabled

Examples > **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	config	Configuration settings.
	trapflags	Trap settings.
	stpmode	Configure spanning tree trap sending.
	{enable disable}	Enable or disable the sending of spanning tree traps.

Defaults	Enabled

Examples	> config trapflags stpmode disable

Related Commands	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	config	Configuration settings.
	trapflags	Trap settings.
	wps	Configure WPS trap sending.
	{enable disable}	Enable or disable WPS trap sending.

Defaults	Enabled

Examples	> config trapflags wps disable

Related Commands	show trapflags

Configure Watchlist Commands

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

config watchlist add

To add a watchlist entry for a wireless LAN, use the **config watchlist add** command.

```
config watchlist add {mac MAC | username username}
```

Syntax Description	config watchlist	Command action.
	add	Add a watchlist entry.
	{mac MAC	• Enter mac and specify the MAC address of the wireless LAN.
	username username}	• Enter username and specify the name of the user to watch.

Defaults	None.

Examples	> config watchlist add mac a5:6b:ac:10:01:6b

Related Commands	config watchlist delete config watchlist enable config watchlist disable show watchlist

config watchlist delete

To delete a watchlist entry for a wireless LAN, use the **config watchlist delete** command.

config watchlist delete {**mac** *MAC* | **username** *username*}

Syntax Description	config watchlist	Command action.
	delete	Delete a watchlist entry.
	{ mac <i>MAC</i> username <i>username</i> }	• Enter mac and specify the MAC address of the wireless LAN to delete from the list.
		• Enter username and specify the name of the user to delete from the list.

Defaults	None.

Examples	> config watchlist delete mac a5:6b:ac:10:01:6b

Related Commands	config watchlist add config watchlist enable config watchlist disable show watchlist

config watchlist disable

To disable the client watchlist, use the **config watchlist disable** command.

config watchlist disable

Syntax Description	config	Command action.
	watchlist	Configure the client watchlist.
	disable	Disable the client watchlist.

Defaults	None.

Examples	> config watchlist disable

Related Commands	config watchlist add config watchlist delete show watchlist

config watchlist enable

To enable a watchlist entry for a wireless LAN, use the **config watchlist enable** command.

config watchlist enable

Syntax Description	config watchlist	Command action.
	watchlist	Configure the client watchlist.
	enable	Enable the client watchlist.

Defaults	None.

Examples	> config watchlist enable

Related Commands	config watchlist add config watchlist delete show watchlist

Configure Wireless LAN Commands

Use the **config wlan** commands to configure wireless LAN command settings.

config wlan

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

config wlan { **enable** | **disable** | **create** | **delete** } *wlan_id* [*name* | **foreignAp** *name ssid* | **all**]

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
enable disable	Enable or disable a wireless LAN.
create delete	Create or delete a wireless LAN.
<i>wlan_id</i>	A wireless LAN identifier between 1 and 512.
<i>name</i>	WLAN profile name up to 32 alphanumeric characters.
foreignAp	Third-party access point settings.
<i>ssid</i>	SSID (network name) up to 32 alphanumeric characters.
all	Include all wireless LANs.

Defaults

None.

Usage Guidelines

When you create a new WLAN using the **config wlan create** command, it is created in disabled mode. Leave it disabled until you have finished configuring it.

If you do not specify an SSID, the profile name parameter is used for both the profile name and the SSID.

If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

Examples

```
> config wlan enable 16
> config wlan create 31 foreignAp thirty1
```

Related Commands

[show ap wlan](#)
[show wlan](#)

config wlan 7920-support

To configure support for phones, use the **config wlan 7920-support** command.

config wlan 7920-support { **client-cac-limit** | **ap-cac-limit** } { **enable** | **disable** } *wlan_id*

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	7920-support	Configure support for phones.
	ap-cac-limit client-cac-limit	- Enter ap-cac-limit to support phones that require client-controlled Call Admission Control (CAC) (that expect the Cisco vendor-specific information element (IE)). - Enter client-cac-limit to support phones that require access point-controlled CAC (that expect the IEEE 802.11e Draft 6 QBSS-load).
	enable disable	Enable or disable phone support.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults None.

Usage Guidelines You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

Examples

```
> config wlan 7920-support ap-cac-limit enable 8
```

Related Commands **show wlan**

config wlan 802.11e

To configure 802.11e support on a wireless LAN, use the **config wlan 802.11e** command.

config wlan 802.11e { **allow** | **disable** | **require** } *wlan_id*

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
802.11e	Configure 802.11e.
allow disable require	- Enter allow to allow 802.11e on the wireless LAN. - Enter disable to disable 802.11e on the wireless LAN. - Enter require to require 802.11e-enabled clients on the wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Usage Guidelines

802.11e provides Quality of Service (QoS) support for LAN applications, which are critical for delay sensitive applications such as Voice over Wireless IP (VoWIP).

802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability and is especially well suited for use in networks that include multimedia capability.

Examples

```
> config wlan 802.11e allow 1
```

Related Commands

show trapflags

config wlan aaa-override

To configure user policy override via AAA on a wireless LAN, use the **config wlan aaa-override** command.

config wlan aaa-override {enable | disable} {wlan_id | foreignAp}

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
aaa-override	Configures user policy override via AAA on a wireless LAN.
enable disable	Enable or disable policy override.
wlan_id foreignAp	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults

Disabled.

Usage Guidelines

When AAA override is enabled, and a client has conflicting AAA and Cisco Wireless LAN controller wireless LAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system will move clients from the default Cisco wireless LAN solution wireless LAN VLAN to a VLAN returned by the AAA server and predefined in the Cisco Wireless LAN controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system will also use QoS, DSCP, 802.1p priority tag values and ACL provided by the AAA server, as long as they are predefined in the Cisco Wireless LAN controller interface configuration. (This VLAN switching by AAA override is also referred to as Identity Networking.)

For instance, if the Corporate wireless LAN primarily uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the Operating System redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.

When AAA override is disabled, all client authentication defaults to the Cisco Wireless LAN controller authentication parameter settings, and authentication is only performed by the AAA server if the Cisco Wireless LAN controller wireless LAN do not contain any client-specific authentication parameters.

The AAA override values may come from a RADIUS server, for example.

Examples

```
> config wlan aaa-override enable 1
```

Related Commands

show wlan

config wlan acl

To configure a wireless LAN access control list (ACL), use the **config wlan acl** command.

```
config wlan acl wlan_id [ acl_name | none ]
```

Syntax Description	wlan_id	Specifies the wireless LAN identifier (1 to 512).
	acl_name	Specifies the ACL name.
	none	Clears the ACL settings for the specified wireless LAN.

Defaults None.

Examples > config wlan acl 1 office_1

Related Commands show wlan

config wlan apgroup

To manage access point group VLAN features, use the **config wlan apgroup** command.

```
config wlan apgroup {add apgroup_name wlan_id interface_name |
  delete apgroup_name |
  description apgroup_name description |
  interface-mapping {add | delete} apgroup_name wlan_id interface_name |
  nac {enable | disable} apgroup_name wlan_id
```

Syntax Description	
config	Configuration settings.
wlan	Wireless LAN settings.
apgroup	Wireless LAN access point group settings.
add	Create a new access point group.
<i>apgroup_name</i>	Access point group name.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>interface_name</i>	The interface to which you want to map the access point group.
description	Describes an access point group.
<i>description</i>	A description of the access point group.
interface-mapping	Assign or remove a Wireless LAN from an access point group.
add delete	- Enter add to assign a Wireless LAN to an access point group. - Enter delete to remove a Wireless LAN from an access point group.
nac	Enable or disable Network Admission Control (NAC) out-of-band support on an access point group.
enable disable	- Enter enable to turn on NAC out-of-band support on an access point group. - Enter disable to turn off NAC out-of-band support on an access point group.

Defaults Disabled.

Usage Guidelines An error message appears if you try to delete an access point group that is used by at least one access point. Before you can delete an AP group in controller software release 6.0, move all APs in this group to another group. The access points are not moved to the default-group access point group as in previous releases. To see the APs, enter the **show wlan apgroups** command. To move APs, enter the **config ap group-name groupname Cisco_AP** command.

Examples > config wlan apgroup nac enable apgroup 4

Related Commands [config guest-lan nac](#)

config wlan nac
debug group
show ap stats
show ap summary
show ap wlan
show nac statistics
show nac summary
show wlan

config wlan broadcast-ssid

To configure an SSID broadcast on a wireless LAN, use the **config wlan broadcast-ssid** command.

config wlan broadcast-ssid {enable | disable} *wlan_id*

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	broadcast-ssid	Configure an SSID broadcast on a wireless LAN.
	enable disable	Enable or disable SSID broadcasts on a wireless LAN.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults	Disabled.

Examples	> config wlan broadcast-ssid enable 1

Related Commands	show wlan

config wlan call-snoop

To enable or disable VoIP snooping for a particular WLAN, use the **config wlan call-snoop** command.

```
config wlan call-snoop { enable | disable } wlan_id
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	call-snoop	Call snooping settings.
	enable disable	Enable or disable VoIP snooping on a wireless LAN.
	wlan_id	Wireless LAN identifier between 1 and 512.

Command Default None.

Examples To enable CHD for WLAN 3, enter this command:
> config wlan chd 3 enable

Related Commands [show wlan](#)
 [show call-control ap](#)
 [show call-control client](#)
 [config wlan](#)

config wlan chd

To enable or disable Coverage Hole Detection (CHD) for a wireless LAN, use the **config wlan chd** command.

config wlan chd *wlan_id* {**enable** | **disable**}

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
chd	Coverage hole detection settings.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
enable disable	Enable or disable SSID broadcasts on a wireless LAN.

Command Default

None.

Examples

To enable CHD for WLAN 3, enter this command:

```
> config wlan chd 3 enable
```

Related Commands

[show wlan](#)
[config ap wlan](#)
[config wlan](#)

config wlan ccx aironet-ie

To enable or disable Aironet information elements (IEs) for a WLAN, use the **config wlan ccx aironet-ie** command:

```
config wlan ccx aironet-ie {enable | disable}
```

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
ccx	Cisco client extension (CCX) settings.
aironet-ie	Aironet information element settings.
enable disable	Enable or disable this command.

Command Default

None.

Examples

To enable Aironet information elements for a WLAN, enter this command:

```
> config wlan ccx aironet-ie enable
```

Related Commands

[config wlan](#)
[config wlan security ckip](#)
[show client detail](#)

config wlan dhcp_server

To configure the internal DHCP server for a wireless LAN, use the **config wlan dhcp_server** command.

config wlan dhcp_server { *wlan_id* | **foreignAp** } *ip_address* [**required**]

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
dhcp_server	Configure internal DHCP server.
<i>wlan_id</i> foreignAp	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.
<i>ip_address</i>	IP Address of the internal DHCP server (this parameter is required).
required	Optionally, specify whether DHCP address assignment is required.

Defaults

None.

Usage Guidelines

The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override. If you enable the override, you can use the show wlan command to verify that the DHCP server has been assigned to the WLAN.

Examples

```
> config wlan dhcp_server 16 10.10.2.1
```

Related Commands

[config dhcp](#)
[config dhcp proxy](#)
[config interface dhcp](#)
[debug dhcp](#)
[debug dhcp service-port](#)
[debug disable-all](#)
[show dhcp](#)
[show dhcp proxy](#)

config wlan diag-channel

To enable the diagnostic channel troubleshooting on a particular WLAN, use the **config wlan diag-channel** command.

```
config wlan diag-channel [ enable | disable ] wlan_id
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	diag-channel	Diagnostic channel troubleshooting settings.
	enable disable	(Optional) Enable or disable the wireless LAN diagnostic channel.
	wlan_id	Specifies the wireless LAN identifier (1 to 512).

Defaults	None.

Examples	> config wlan diag-channel enable 1

Related Commands	show run-config show wlan

config wlan dtim

To disable a wireless LAN, use the **config wlan disable** command.

```
config wlan dtim { 802.11a | 802.11b } dtim wlan_id
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	dtim	Delivery traffic indication map.
	802.11a 802.11b	- Configure DTIM for 802.11a radio network. - Configure DTIM for 802.11b radio network.
	<i>dtim</i>	Value for DTIM (between 1 - 255 inclusive)
	<i>wlan_id</i>	Number of the WLAN to be configured

Defaults	Default DTIM 1.

Examples	> config wlan dtim 802.11a 128 1

Related Commands	show wlan

config wlan exclusionlist

To configure the wireless LAN exclusion list, use the config wlan exclusionlist command.

```
config wlan exclusionlist [wlan_id [enabled | disabled | time] |
foreignAp [enabled | disabled | time]
```

Syntax Description	<i>wlan_id</i>	Specifies the wireless LAN identifier (1 to 512).
	enabled	Enables the exclusion list for the specified wireless LAN or foreign access point.
	disabled	Disables the exclusion list for the specified wireless LAN, or a foreign access point.
	<i>time</i>	Specifies the exclusion list timeout in seconds. A value of zero (0) specifies infinite time.
	foreignAp	Specifies a third party access point.

Defaults	None.

Usage Guidelines	This command replaces config wlan blacklist .

Examples	> config wlan exclusionlist 1 enabled

Related Commands	show wlan
	show wlan summary

config wlan h-reap learn-ipaddr

To enable or disable client IP address learning for the Cisco WLAN controller, use the **config wlan h-reap learn-ipaddr** command.

config wlan h-reap learn-ipaddr *wlan_id* {**enable** | **disable**}

Syntax Description		
config		Configuration settings.
wlan		Wireless LAN settings.
h-reap		Hybrid REAP parameters.
learn-ipaddr		Client IP address learning feature.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.
enable disable		Enable or disable client IP address learning on a wireless LAN.

Defaults

Disabled when [config wlan h-reap local-switching](#) command is disabled.
 Enabled when [config wlan h-reap local-switching](#) command is enabled. See usage guidelines for more information.

Usage Guidelines

If the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller will periodically drop the client. Disable this option to keep the client connection without waiting to learn the client IP address.



Note The ability to disable IP Address learning is not supported with H-REAP *central* switching.

Examples

To disable client IP address learning for WLAN 6, enter the following command:

```
> config wlan h-reap learn-ipaddr disable 6
```

Related Commands

[config wlan h-reap local-switching](#)
[show wlan](#)

config wlan h-reap local-switching

To configure the WLAN for local switching, use the **config wlan h-reap local switching** command.

config wlan h-reap local-switching {enable | disable} *wlan_id*

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
h-reap	Hybrid-REAP (HREAP) parameters.
local-switching	Local data packet switching feature.
enable disable	Enable or disable local switching on a wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

Disabled.

Usage Guidelines

When you enable **config wlan h-reap local-switching**, the [config wlan h-reap learn-ipaddr](#) command is enabled by default.



Note The ability to disable IP Address learning is not supported with HREAP *central* switching.

Examples

To enable WLAN 6 for local switching, enter the following command:

```
> config wlan h-reap local-switching enable 6
```

Related Commands

[config wlan h-reap learn-ipaddr](#)
[show wlan](#)

config wlan interface

To configure a wireless LAN interface, use the **config wlan interface** command.

config wlan interface { *wlan_id* | **foreignAp** } *interface-name*

Syntax Description	<i>wlan_id</i>	(Optional) Specifies the wireless LAN identifier (1 to 512)
	foreignAp	(Optional) Specifies third party access points.
	<i>interface-name</i>	Specifies the interface name.

Defaults	None.

Examples	> config wlan interface 16 VLAN901

Related Commands	show wlan

config wlan IPv6Support

To configure IPv6 support on a wireless LAN, use the **config wlan IPv6Support** command.

```
config wlan IPv6support {enable | disable} wlan_id
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	IPv6support	Configure IPv6 support on a wireless LAN.
	enable disable	Enable or disable IPv6 support on a wireless LAN.
	wlan_id	Wireless LAN identifier between 1 and 512.

Defaults None.

Examples > config wlan IPv6support enable 6

Related Commands show wlan

config wlan ldap

To add or delete a link to a configured LDAP server, enter the config wlan ldap command.

config wlan ldap {add wlan_id server_id | delete wlan_id {all | server_id}}

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	ldap	Configure the LDAP server priority for the wireless LAN.
	add	Add a link to a configured LDAP server.
	delete	Remove the link to a configured LDAP server.
	<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 512.
	<i>server_id</i>	Enter a LDAP server index.
	all	All LDAP servers.

Defaults None.

Usage Guidelines Use this command to specify the LDAP server priority for the WLAN.

To specify the LDAP server priority, one of the following must be configured and enabled:

- 802.1x authentication and Local EAP
- Web authentication and LDAP



Note Local EAP was introduced in controller software release 4.1; LDAP support on Web authentication was introduced in controller software release 4.2.

Examples

```
> config wlan ldap add 100 4
> config wlan ldap delete all
```

Related Commands [config ldap](#)

config wlan load-balance

To override the global load balance configuration and enable or disable load balancing on a particular WLAN, enter the **config wlan load-balance** command.

```
config wlan load-balance allow {enable | disable} wlan_id
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	load-balance allow	Load balance mode.
	enable disable	Enable or disable band selection on a wireless LAN.
	wlan_id	Wireless LAN identifier between 1 and 512.

Defaults Enabled.

Examples > config wlan load-balance allow disable 3

Related Commands [config load-balancing](#)

config wlan mac-filtering

To change the state of MAC filtering on a wireless LAN, use the **config wlan mac-filtering** command.

config wlan mac-filtering {enable | disable} {wlan_id | foreignAp}

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	mac-filtering	Configure MAC filtering on a wireless LAN.
	{enable disable}	Enable or disable MAC filtering on a wireless LAN.
	{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults	None.

Examples	> config wlan mac-filtering enable 1

Related Commands	show wlan

config wlan mfp

To configure management frame protection (MFP) options for the wireless LAN, use the **config wlan mfp** command.

```
config wlan mfp {client [enable | disable ] wlan_id |
infrastructure protection [ enable | disable ] wlan_id }
```

Syntax Description	client	(Optional) Configures client MFP for the wireless LAN.
	enable	Enables the feature.
	disable	Disables the feature.
	wlan_id	Specifies the wireless LAN identifier (1 to 512).
	infrastructure protection	(Optional) Configures infrastructure MFP for the wireless LAN.

Defaults None.

Examples > config wlan mfp client enable 1

Related Commands show run-config
show wlan summary
show wlan

config wlan mobility anchor

To change the state of MAC filtering on a wireless LAN, use the **config wlan mobility anchor** command.

config wlan mobility anchor {add | delete} *wlan_id ip_address*

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	mobility anchor	Configure the Mobility wireless LAN anchor list.
	add delete	Enable or disable MAC filtering on a wireless LAN.
	<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 512.
	<i>ip_address</i>	Member switch IP address for anchoring the wireless LAN.

Defaults None.

Examples
 > config wlan mobility anchor add 4 192.168.0.14

Related Commands

- config guest-lan mobility 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 mobility statistics reset
- debug mobility
- show mobility anchor
- show mobility statistics
- show mobility summary

config wlan nac

To enable or disable NAC out-of-band support for a WLAN, enter this command:

```
config wlan nac {enable | disable} wlan_id
```

Syntax Description

config	Command action.
wlan	WLAN parameters.
nac	NAC out-of-band support.
enable disable	Enable or disable NAC out-of-band support.
<i>wlan_id</i>	The WLAN identifier between 1 and 512.

Defaults

None

Examples

```
>config wlan nac enable 13
```

Related Commands

[show nac statistics](#)
[show nac summary](#)
[config guest-lan nac](#)
[debug nac](#)

config wlan peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **config wlan peer-blocking** command.

config wlan peer-blocking { **disable** | **drop** | **forward-upstream** } *wlan_id*

Syntax Description	config	Configuration settings.
	wlan	WLAN parameters.
	peer-blocking	Configures a WLAN for peer-to-peer blocking.
	{ disable drop forward-upstream }	- Enter disable to disable peer-to-peer blocking and bridge traffic locally within the controller whenever possible. - Enter drop to cause the controller to discard the packets. - Enter forward-upstream to cause the packets to be forwarded on the upstream VLAN. The device above the controller decides what action to take regarding the packets.
	<i>wlan_id</i>	The WLAN identifier between 1 and 512.

Defaults **config wlan peer-blocking disable** *wlan_id*

Examples
 > **config wlan peer-blocking disable 1**

Related Commands **show wlan**

config wlan qos

To change the quality of service for a wireless LAN, use the **config wlan qos** command.

```
config wlan qos wlan_id {bronze | silver | gold | platinum}

config wlan qos foreignAp {bronze | silver | gold | platinum}
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	qos	Quality of service.
	wlan_id	Wireless LAN identifier between 1 and 512.
	foreignAp	Enter foreignAp for third party access points.
	{bronze silver gold platinum}	Enter QoS policy: bronze , silver , gold , or platinum .

Defaults Silver.

Examples To set the highest level of service on wireless LAN 1, use the following command:

```
> config wlan qos 1 gold
```

Related Commands show wlan

config wlan radio

To set the Cisco radio policy on a wireless LAN, use the **config wlan radio** command.

config wlan radio *wlan_id* {**all** | **802.11a** | **802.11bg** | **802.11g** | **802.11ag**}

Syntax Description	
config	Configuration settings.
wlan	Wireless LAN settings.
radio	Configure the Cisco radio policy.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
{ all 802.11a 802.11bg 802.11g 802.11ag }	- Enter all to configure the wireless LAN on all radio bands. - Enter 802.11a to configure the wireless LAN on only 802.11a. - Enter 802.11bg to configure the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled). - Enter 802.11g to configure the wireless LAN on 802.11g only. - Enter 802.11ag to configure the wireless LAN on 802.11a and 802.11g only.

Defaults None.

Examples
 > config wlan radio 1 all

Related Commands

```

config 802.11a enable
config 802.11a disable
config 802.11b enable
config 802.11b disable
config 802.11b 11gSupport enable
config 802.11b 11gSupport disable
show wlan

```

config wlan radius_server

To configure a wireless LAN's radius servers, use the **config wlan radius_server** command.

```
config wlan radius_server {auth | acct} {enable wlan_id | disable wlan_id} {add wlan_id
server_id | delete wlan_id {all | server_id}}
```

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
radius-server	RADIUS servers.
{auth acct}	Configures a RADIUS authentication or accounting server.
{enable disable}	Enable or disable RADIUS authentication or accounting for this WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
{add delete}	Add or delete a link to a configured RADIUS Server.
<i>server_id</i>	RADIUS Server Index.
all	Enter all to delete all links to configured RADIUS servers.

Defaults

None.

Examples

```
> config wlan radius_server auth add 1 1
> config wlan radius_server auth delete 1 1
> config wlan radius_server auth delete 1 all
```

Related Commands

```
config 802.11a enable
config 802.11a disable
config 802.11b enable
config 802.11b disable
config 802.11b 11gSupport enable
config 802.11b 11gSupport disable
show wlan
```

Configure Wireless LAN Security Commands

Use the **config wlan security** commands to configure wireless LAN security settings.

config wlan security 802.1X

To change the state of 802.1X security on the wireless LAN Cisco radios, use the **config wlan security 802.1X** command.

```
config wlan security 802.1X {enable {wlan_id | foreignAp} | disable {wlan_id | foreignAp} |
  encryption {wlan_id | foreignAp} {0 | 40 | 104}}
```

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
security	Configure the wireless LAN security policy.
802.1X	Configure 802.1X security.
{ enable disable encryption }	- Enter disable to disable 802.1X. - Enter enable to enable 802.1X. - Enter encryption to set the static WEP keys and indexes.
{ <i>wlan_id</i> foreignAp }	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.
{ 0 40 104 }	If you're setting the static WEP keys and indexes using the config wlan security 802.1X encryption command, enter a WEP key size of 0 (no encryption), 40, or 104 bits. The default value is 104.
	
Note	All keys within a wireless LAN must be same size.

Defaults

None.

Usage Guidelines

Use to change the encryption level of 802.1X security on the wireless LAN Cisco radios to:

- 0—no 802.1X encryption.
- 40—40/64-bit encryption.
- 104—104/128-bit encryption. (This is the default encryption setting.)

Examples

```
> config wlan security 802.1X enable 16
```

Related Commands

show wlan

config wlan security ckip

To configure Cisco Key Integrity Protocol (CKIP) security options for the wireless LAN, use the **config wlan security ckip** command.

```
config wlan security ckip {enable | disable} wlan_id
    [akm psk set-key {hex | ascii} {40 | 104} key key_index wlan_id |
    mmh-mic {enable | disable} wlan_id |
    kp {enable | disable} wlan_id]
```

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
security	Configure the wireless LAN security policy.
ckip	Cisco Key Integrity Protocol settings.
enable disable	Enable or disable CKIP security.
wlan_id	The WLAN to which you apply the command.
akm psk set-key	(Optional) Configures encryption key management for the CKIP wireless LAN.
hex ascii	- Enter hex to specify a hexadecimal encryption key. - Enter ascii to specify an ASCII encryption key.
40 104	- Enter 40 to set the static encryption key length to 40 bits for the CKIP WLAN. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. - Enter 104 to set the static encryption key length to 104 bits for the CKIP WLAN. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.
key	CKIP WLAN key settings.
key_index	The configured PSK key index.
mmh-mic	(Optional) Configures multi-modular hash message integrity check (MMH MIC) validation for the CKIP wireless LAN.
kp	(Optional) Configures key-permutation for the CKIP wireless LAN.

Defaults

None.

Examples

To configure a CKIP WLAN encryption key of 104 bits (26 hexadecimal characters) for PSK key index 2 on WLAN 03, enter this command:

```
> config wlan security ckip akm psk set-key hex 104 key 2 03
```

Related Commands

[config wlan ccx aironet-ie](#)
[show wlan](#)

config wlan security cond-web-redir

To enable or disable conditional web redirect, enter this command.

```
config wlan security cond-web-redir {enable | disable} wlan_id
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	cond-web-redir	Configure conditional web redirect
	{enable disable}	- Enter enable to enable conditional web redirect. - Enter disable to disable conditional web redirect.
	<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 512.

Defaults	None.

Examples	> config wlan security cond-web-redir enable 2

Related Commands	show wlan show wlan <i>wlan_id</i> .

config wlan security ipsec disable

To disable IPSec security, use the **config wlan security ipsec disable** command.

```
config wlan security ipsec disable {wlan_id | foreignAp}
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	ipsec disable	Disable IPSec.
	wlan_id foreignAp	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults None.

Examples > config wlan security IPSec disable 16

Related Commands show wlan

config wlan security ipsec enable

To enable IPSec security, use the **config wlan security ipsec enable** command.

config wlan security ipsec enable {*wlan_id* | **foreignAp**}

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	ipsec enable	Enable IPSec.
	<i>wlan_id</i> foreignAp	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults	None.

Examples	> config wlan security IPSec enable 16

Related Commands	show wlan

config wlan security ipsec authentication

To modify the IPSec security authentication protocol used on the wireless LAN, use the **config wlan security ipsec authentication** command.

config wlan security ipsec authentication { hmac-md5 | hmac-sha-1 } { wlan_id | foreignAp }

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
security	Configure the wireless LAN security policy.
ipsec authentication	Configure IPSec security authentication parameter.
{hmac-md5 hmac-sha-1}	Enter the IPSec HMAC-MD5 or IPSec HMAC-SHA-1 authentication protocol.
wlan_id foreignAp	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults

None.

Examples

```
> config wlan security ipsec authentication hmac-sha-1 1
```

Related Commands

show wlan

config wlan security ipsec encryption

To modify the IPSec security encryption protocol used on the wireless LAN, use the **config wlan security ipsec encryption** command.

config wlan security ipsec encryption {3des | aes | des} {wlan_id | foreignAp}

Syntax Description		
config		Configuration settings.
wlan		Wireless LAN settings.
security		Configure the wireless LAN security policy.
ipsec		IPSec security.
encryption		Encryption parameter.
{3des aes des}		Enable IPSec DES encryption, IPSec AES 128-bit encryption, or IPSec 3DES encryption.
wlan_id foreignAp		- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults None.

Examples > **config wlan security ipsec encryption aes 1**

Related Commands **show wlan**

config wlan security ipsec config

To configure the propriety IKE CFG-Mode parameters used on the wireless LAN, use the **config wlan security ipsec config** command.

IKE is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how the data should be protected. IKE keeps track of connections by assigning a bundle of Security Associations (SAs), to each connection.

config wlan security ipsec config qotd *ip_address* {*wlan_id* | **foreignAp}**

Syntax Description

config	Configuration settings.
wlan	Configure Wireless LAN settings.
security	Configure the wireless LAN security policy.
ipsec	Configure IPSec security.
config	Configure proprietary IKE CFG-MODE parameters.
qotd	Configure quote-of-the-day server IP for cfg-mode.
<i>ip_address</i>	quote-of-the-day server IP for cfg-mode.
<i>wlan_id</i> foreignAp	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults

None.

Examples

```
> config wlan security ipsec config qotd 44.55.66.77 1
```

Related Commands

show wlan

config wlan security ipsec ike authentication

To modify the IPSec ike authentication protocol used on the wireless LAN, use the **config wlan security ipsec ike authentication** command.

```
config wlan security ipsec ike authentication {certificates {wlan_id | foreignAp} |  
  pre-share-key {wlan_id | foreignAp} key | xauth-psk {wlan_id | foreignAp} key}
```

Syntax	Description
config	Configuration settings.
wlan	Wireless LAN settings.
security	Configure the wireless LAN security policy.
ipsec	IPSec security.
ike	IKE protocol.
authentication	Authentication parameter.
{ certificates pre-share-key xauth-psk }	- Enter certificates to enable IKE certificate mode. - Enter pre-share-key to enable IKE Xauth with pre-shared keys. - Enter xauth-psk to enable IKE Pre-Shared Key.
<i>wlan_id</i> foreignAp	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.
<i>key</i>	Key required for pre-share and xauth-psk.

Defaults None.

Examples > **config wlan security ipsec ike authentication certificates 16**

Related Commands **show wlan**

config wlan security ipsec ike dh-group

To modify the IPSec IKE Diffie Hellman group used on the wireless LAN, use the **config wlan security ipsec ike authentication** command.

```
config wlan security ipsec ike dh-group { wlan_id | foreignAp } { group-1 | group-2 | group-5 }
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	ipsec	Configure IPSec security.
	ike	Configure the IKE protocol.
	dh-group	Diffie Hellman group parameter.
	wlan_id foreignAp	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.
	{group-1 group-2 group-5}	- Enter group-1 to specify DH group 1 (768 bits). - Enter group-2 to specify DH group 2 (1024 bits). - Enter group-5 to specify DH group 5 (1536 bits).

Defaults None.

Examples > config wlan security ipsec ike dh-group 1 group-1

Related Commands show wlan

config wlan security ipsec ike lifetime

To modify the IPSec IKE lifetime used on the wireless LAN, use the **config wlan security ipsec ike lifetime** command.

config wlan security ipsec ike lifetime {*wlan_id* | **foreignAp**} *seconds*

Syntax Description		
config		Configuration settings.
wlan		Configure Wireless LAN settings.
security		Configure the wireless LAN security policy.
ipsec		Configure IPSec security.
ike		Configure IKE protocol.
lifetime		Configure IKE timeout.
<i>wlan_id</i> foreignAp		- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.
<i>seconds</i>		The IKE lifetime in seconds, between 1800 and 345600.

Defaults None.

Examples > **config wlan security ipsec ike lifetime 1 1900**

Related Commands **show wlan**

config wlan security ipsec ike phase1

To modify IPSec IKE Phase 1 used on the wireless LAN, use the **config wlan security ipsec ike phase1** command.

```
config wlan security ipsec ike phase1 {aggressive | main} {wlan_id | foreignAp}
```

Syntax Description	config	Configuration settings.
	wlan	Configure Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	ipsec	Configure IPSec security.
	ike	Configure IKE.
	phase1	Configure IKE's phase one mode.
	aggressive main	- Enter aggressive to enable the IKE aggressive mode. - Enter main to enable the IKE main mode.
	wlan_id foreignAp	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults None.

Examples > config wlan security ipsec ike phase1 aggressive 16

Related Commands show wlan

config wlan security ipsec ike contivity

To modify Nortel's Contivity VPN client support on the wireless LAN, use the **config wlan security ipsec ike contivity** command.

config wlan security ipsec ike contivity {enable | disable} {wlan_id | foreignAp}

Syntax Description		
config		Configuration settings.
wlan		Configure Wireless LAN settings.
security		Configure the wireless LAN security policy.
ipsec		Configure IPSec security.
ike		Configure IKE protocol.
contivity		Configure Nortel Contivity VPN client support.
{enable disable}		Enable or disable contivity support for this wlan.
wlan_id foreignAp		- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults None.

Examples > **config wlan security ipsec ike contivity enable 14**

Related Commands **show wlan**

config wlan security passthru

To modify the IPSec pass-through used on the wireless LAN, use the **config wlan security ipsec ike passthru** command.

```
config wlan security passthru {enable | disable} {wlan_id | foreignAp} [ip_address]
```

Syntax Description

config	Configuration settings.
wlan	Configure Wireless LAN settings.
security	Configure the wireless LAN security policy.
passthru	Configure IPSec pass-through.
enable disable	Enable or disable IPSec pass-through.
wlan_id foreignAp	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.
ip_address	If you enable security pass-through, you must specify the IP address of the IPSec gateway (router) that is terminating the VPN tunnel.

Defaults

None.

Examples

```
> config wlan security passthru enable 3 192.12.1.1
```

Related Commands

show wlan

config wlan security splash-page-web-redir

To enable or disable splash page web redirect, enter this command.

```
config wlan security splash-page-web-redir {enable | disable} wlan_id
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	splash-page-web-redir	Configure splash page web redirect
	{enable disable}	- Enter enable to enable splash page web redirect. - Enter disable to disable splash page web redirect.
	<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 512.

Defaults	Disabled.

Examples	> config wlan security splash-page-web-redir enable 2

Related Commands	show wlan

config wlan security static-wep-key authentication

To configure static WEP key 802.11 authentication on a wireless LAN, use the **config wlan security static-wep-key authentication** command.

```
config wlan security static-wep-key authentication {shared-key | open} wlan_id
```

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
security	Configure the wireless LAN security policy.
static-wep-key	Configure static WEP keys on a wireless LAN.
authentication	Authentication setting.
{shared-key open}	- Enter shared-key to enable shared key authentication. - Enter open to enable open system authentication.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

```
> config wlan security static-wep-key authentication shared-key 1
> config wlan security static-wep-key authentication open 1
```

Related Commands

show wlan

config wlan security static-wep-key disable

To disable the use of static WEP keys, use the **config wlan security static-wep-key disable** command.

config wlan security static-wep-key disable *wlan_id*

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	static-wep-key	Configure static WEP keys on a wireless LAN.
	disable	Disable the use of static WEP keys.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults None.

Examples

```
> config wlan security static-wep-key disable 1
```

Related Commands **config wlan security wpa encryption**

config wlan security static-wep-key enable

To enable the use of static WEP keys, use the **config wlan security static-wep-key enable** command.

```
config wlan security static-wep-key enable wlan_id
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	static-wep-key	Configure static WEP keys on a wireless LAN.
	enable	Disable the use of static WEP keys.
	wlan_id	Wireless LAN identifier between 1 and 512.

Defaults None.

Examples > config wlan security static-wep-key enable 1

Related Commands config wlan security wpa encryption

config wlan security static-wep-key encryption

To configure the static WEP keys and indexes, use the **config wlan security static-wep-key encryption** command. Make sure to disable 802.1X before using this command.

config wlan security static-wep-key encryption *wlan_id* { **40** | **104** } { **hex** | **ascii** } *key* *key-index*

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	static-wep-key	Configure static WEP keys on a wireless LAN.
	encryption	Encryption setting.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	{ 40 104 }	Encryption level.
	{ hex ascii }	Specify whether to use hexadecimal or ASCII characters to enter key.
	<i>key</i>	Enter WEP key in ascii
	<i>key-index</i>	Key index (1 to 4).

Defaults None.

Usage Guidelines One unique WEP Key Index can be applied to each wireless LAN. As there are only four WEP Key Indexes, only four wireless LANs can be configured for Static WEP Layer 2 encryption.

Examples

```
> config wlan security static-wep-key encryption 1 40 hex 0201702001 2
```

Related Commands `show wlan`

config wlan security web-auth

To change the status of Web authentication used on the wireless LAN, use the **config wlan security web** command.

```
config wlan security web-auth {acl | enable | disable} {wlan_id | foreignAp} [acl_name | none]
```

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
security	Configure the wireless LAN security policy.
web-auth	Web authentication.
acl enable disable	Configure the Access Control List, or enable or disable web authentication.
wlan_id foreignAp	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.
acl_name none	If configuring an ACL, enter the ACL name (up to 32 alphanumeric characters) or none .

Defaults

None.

Examples

```
> config wlan security web-auth acl 1 ACL03
> config wlan security web-auth enable 1
> config wlan security web-auth disable 1
```

Related Commands

[show wlan](#)

config wlan security web-passthrough acl

To add an ACL to the wireless LAN definition, use the **config wlan security web acl** command.

config wlan security web-passthrough acl {*wlan_id* | **foreignAp**} {*acl_name* | **none**}

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	web-passthrough	Configure the web captive portal with no authentication required.
	acl	Add an ACL to the wireless LAN definition.
	{ <i>wlan_id</i> foreignAp }	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.
	{ <i>acl_name</i> none }	Enter the ACL name (up to 32 alphanumeric characters) or none .

Defaults None.

Examples > **config wlan security web-passthrough acl 1 ACL03**

Related Commands **show wlan**

config wlan security web-passthrough disable

To disable web captive portal with no authentication required on a wireless LAN, use the **config wlan security web-passthrough disable** command.

```
config wlan security web-passthrough disable {wlan_id | foreignAp}
```

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
security	Configure the wireless LAN security policy.
web-passthrough	Configure the web captive portal with no authentication required.
disable	Disable web captive portal with no authentication required.
{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults

None.

Examples

```
> config wlan security web-passthrough disable 1
```

Related Commands

show wlan

config wlan security web-passthrough email-input

To configure web captive portal using an email address, use the **config wlan security web-passthrough email-input** command.

```
config wlan security web-passthrough email-input {enable | disable} {wlan_id | foreignAp}
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	web-passthrough	Configure the web captive portal with no authentication required.
	email-input	Configure web captive portal using an email address.
	{enable disable}	Enable or disable web captive portal using email address.
	{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults
None.

Examples
> config wlan security web-passthrough email-input enable 1

Related Commands
show wlan

config wlan security web-passthrough enable

To enable web captive portal with no authentication required on the wireless LAN, use the **config wlan security web-passthrough enable** command.

```
config wlan security web-passthrough enable {wlan_id | foreignAp}
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	web-passthrough	Configure the web captive portal with no authentication required.
	enable	Enable web captive portal with no authentication required.
	{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.

Defaults	None.

Examples	> config wlan security web-passthrough enable 1

Related Commands	show wlan

config wlan security wpa1 disable

To disable WPA1, use the **config wlan security wpa1 disable** command.

config wlan security wpa1 disable *wlan_id*

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	wpa1	Configure WiFi protected access.
	disable	Disable WPA1.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults	None.

Examples	> config wlan security wpa1 disable 1

Related Commands	show wlan

config wlan security wpa1 enable

To enable WPA1, use the **config wlan security wpa1 enable** command.

config wlan security wpa1 enable *wlan_id*

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
security	Configure the wireless LAN security policy.
wpa1	Configure WiFi protected access.
enable	Enable WPA1.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

```
> config wlan security wpa1 enable 1
```

Related Commands

show wlan

config wlan security wpa1 pre-shared-key

To configure the WPA pre-shared key mode, use the **config wlan security wpa1 pre-shared-key** command.

```
config wlan security wpa1 pre-shared-key {enable wlan_id key | disable wlan_id}
```

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
security	Configure the wireless LAN security policy.
wpa1	Configure WiFi protected access.
pre-shared-key	Configure WPA pre-shared key mode (WPA-PSK).
{enable disable}	Enable or disable WPA-PSK.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>key</i>	WPA pre-shared key.

Defaults

None.

Examples

```
> config wlan security wpa1 pre-shared-key enable 1 r45
```

Related Commands

show wlan

config wlan security wpa2 disable

To disable WPA2, use the **config wlan security wpa2 disable** command.

config wlan security wpa2 disable *wlan_id*

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
security	Configure the wireless LAN security policy.
wpa2	Configure WPA2.
disable	Disable WPA2
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

```
> config wlan security wpa2 disable 1
```

Related Commands

show wlan

config wlan security wpa2 enable

To enable WPA2, use the **config wlan security wpa2 enable** command.

config wlan security wpa2 enable *wlan_id*

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	wpa2	Configure WPA2.
	enable	Enable WPA2
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults None.

Examples > **config wlan security wpa2 enable 1**

Related Commands **show wlan**

config wlan security wpa2 pre-shared-key

To configure the WPA pre-shared key mode, use the **config wlan security wpa2 pre-shared-key** command.

```
config wlan security wpa2 pre-shared-key {enable wlan_id key | disable wlan_id}
```

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
security	Configure the wireless LAN security policy.
wpa2	Configure WPA2.
pre-shared-key	Configure WPA2 pre-shared key mode (WPA2-PSK).
{enable disable}	Enable or disable WPA2-PSK.
wlan_id	Wireless LAN identifier between 1 and 512.
key	WPA pre-shared key.

Defaults

None.

Examples

```
> config wlan security wpa2 pre-shared-key disable 2
```

Related Commands

show wlan

config wlan security wpa2 tkip

To change the status of WPA authentication, use the **config wlan security wpa2 tkip** command.

config wlan security wpa2 tkip {enable | disable} wlan_id

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	wpa2	Configure WPA2.
	tkip	Configure WPA2 TKIP mode.
	{enable disable}	Enable or disable the WPA2 TKIP mode.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults None.

Examples
> **config wlan security wpa2 tkip enable 1**

Related Commands **show wlan**

config wlan security wpa2 wpa-compat

To change the status of WPA authentication, use the **config wlan security wpa2 wpa-compat** command.

```
config wlan security wpa2 wpa-compat {enable | disable} wlan_id
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	security	Configure the wireless LAN security policy.
	wpa2	Configure WPA2.
	wpa-compat	Configure WPA compatibility mode.
	{enable disable}	Enable or disable WPA compatibility mode.
	wlan_id	Wireless LAN identifier between 1 and 512.

Defaults None.

Examples > config wlan security wpa2 wpa-compat enable 1

Related Commands show wlan

config wlan timeout

To change the timeout of wireless LAN clients, use the **config wlan timeout** command.

config wlan timeout {*wlan_id* | **foreignAp**} *seconds*

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	timeout	Configure client timeout.
	{ <i>wlan_id</i> foreignAp }	- Enter a wireless LAN identifier between 1 and 512. - Enter foreignAp for third party access points.
	<i>seconds</i>	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

None.

Examples

```
> config wlan timeout 1 6000
```

Related Commands

show wlan

config wlan webauth-exclude

To release the guest user IP address when the Web authentication policy time expires and exclude the guest user from acquiring an IP address for three minutes, use the **config wlan webauth-exclude** command.

config wlan webauth-exclude *wlan_id* {**enable** | **disable**}

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
webauth-exclude	Web authentication exclusion.
<i>wlan_id</i>	Specifies the wireless LAN identifier (1 to 512).
enable	Enable Web authentication exclusion.
disable	Disable Web authentication exclusion.

Command Default

Disabled.

Usage Guidelines

You can use this command for guest WLANs that are configured with Web authentication.

This command is applicable when you configure the internal DHCP scope on the controller.

By default, when the Web authentication timer expires for a guest user, the guest user can immediately reassociate with the same IP address before another guest user can acquire the IP address. If there are many guest users or limited IP address in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user's IP address is released when the Web authentication policy time expires and the guest user is excluded from acquiring an IP address for three minutes. The IP address is available for another guest user to use. After three minutes, the excluded guest user can reassociate and acquire an IP address, if available.

Examples

```
> config wlan webauth-exclude 5 enable
```

Related Commands

[config dhcp](#)

[show run-config](#)

[show wlan](#)

config wlan wmm

To configure Wi-Fi Multimedia (WMM) mode on a wireless LAN, use the **config wlan wmm** command.

config wlan wmm [**allow** | **disable** | **require**] *wlan_id*

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	wmm	Wi-Fi multimedia mode settings.
	allow	(Optional) Allows WMM on the wireless LAN.
	<i>wlan_id</i>	Specifies the wireless LAN identifier (1 to 512).
	disable	(Optional) Disables WMM on the wireless LAN.
	require	(Optional) Requires clients to use WMM on the specified wireless LAN.

Command Default None.

Usage Guidelines When the controller is in Layer 2 mode and WMM is enabled, you must put the access points on a trunk port in order to allow them to join the controller.

Examples

```
> config wlan wmm allow 1
> config wlan wmm require 1
```

Related Commands

```
show run-config
show wlan
```

Configure WPS Commands

Use the **config wps** commands to configure Wireless Protection Services (WPS) settings.

config wps ap-authentication

To configure access point neighbor authentication, use the **config wps ap-authentication** command.

config wps ap-authentication [**enable** | **disable** | **threshold** *threshold_value*]

Syntax Description

enable	(Optional) Enables WMM on the wireless LAN.
disable	(Optional) Disables WMM on the wireless LAN.
threshold	(Optional) Requires WMM enabled clients on the wireless LAN.
<i>threshold_value</i>	Specifies the threshold value (1 to 255).

Command Default

None.

Examples

```
> config wps ap-authentication threshold 25
> config wps ap-authentication enable

> show wps ap-authentication summary

AP neighbor authentication is <enabled>.

Authentication alarm threshold is 10.
RF-Network Name: <doc>

> config wps ap-authentication disable

> show wps ap-authentication summary

AP neighbor authentication is <disabled>.

Authentication alarm threshold is 10.
RF-Network Name: <doc>
```

Related Commands

show wps ap-authentication summary

config wps auto-immune

To enable or disable protection from DoS attacks, use the **config wps auto-immune** command.

```
config wps auto-immune {enable | disable}
```

Syntax Description

auto-immune	Auto-immune mode.
enable disable	Enable or disable auto-immune.

Command Default

Disabled.

Usage Guidelines

A potential attacker can use specially crafted packets to mislead the IDS into treating a legitimate client as an attacker. It causes the controller to wrongly disconnect this legitimate client and launches a DoS attack. The auto-immune feature, when enabled, is designed to protect against such attacks. However, conversations using Cisco 792x phones might be interrupted intermittently when the auto-immune feature is enabled. If you experience frequent disruptions when using 792x phones, you might want to disable this feature.

Examples

```
> config wps auto-immune enable
```

Related Commands

[show wps summary](#)

config wps cids-sensor

This command is used to configure Intrusion Detection System (IDS) sensors for the WPS, use the **config wps cids-sensor** command.

```
config wps cids-sensor { [ add index ip_address username password ] | [delete index] |
[enable index] | [disable index] | [port index port] | [interval index query_interval] |
[fingerprint index sha1 fingerprint]}
```

Syntax	Description
add	Configures a new IDS sensor.
<i>index</i>	Specifies IDS sensor internal index.
<i>ip_address</i>	Specifies the IDS sensor IP address.
<i>username</i>	Specifies the IDS sensor username.
<i>password</i>	Specifies the IDS sensor password.
delete	Deletes an IDS sensor.
enable	Enables an IDS sensor.
disable	Disables an IDS sensor.
port	Configures the IDS sensor's port number.
<i>port</i>	Specifies the port number.
interval	Configures the IDS sensor's query interval.
<i>query_interval</i>	Specifies the query interval setting.
fingerprint	Configures the IDS sensor's TLS fingerprint.
sha1	Configures the TLS fingerprint.
<i>fingerprint</i>	Specifies the TLS fingerprint.

Command Default	Command defaults are listed below:	
	Port	443
	Query interval	60
	Certification fingerprint	00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
	Query state	Disabled

Examples

```
> config wps cids-sensor add 1 10.0.0.51 Sensor_user0doc1 password01
```

Related Commands `show wps cids-sens``show wps cids-sensor detail`

config wps client-exclusion

To configure configure client exclusion policies, use the **config wps client-exclusion** command.

```
config wps client-exclusion {802.11-assoc | 802.11-auth | 802.1x-auth | ip-theft | web-auth | all}
{enable | disable}
```

Syntax Description	client-exclusion	Client exclusion policies.
	802.11-assoc	The controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
	802.11-auth	The controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
	802.1x-auth	The controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
	ip-theft	The controller excludes clients if the IP address is already assigned to another device.
	web-auth	The controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
	all	The controller excludes clients for all of the above reasons.
	enable disable	Enable or disable client exclusion policies.

Defaults All policies are enabled.

Examples

```
> config wps client-exclusion 802.11-assoc disable
```

Related Commands [show wps summary](#)

config wps mfp

To configure Management Frame Protection (MFP), use the **config wps mfp** command.

```
config wps mfp infrastructure {enable | disable}
```

Syntax Description	mfp infrastructure	Configures infrastructure MFP.
	enable disable	Enable or disable MFP.

Defaults	None.

Examples	> config wps mfp infrastructure enable
	> config wps mfp infrastructure disable

Related Commands	show wps mfp

config wps shun-list

To force the controller to sync up with other controllers in the mobility group for the shun list, enter this command:

config wps shun-list re-sync

Syntax Description	This command has no arguments or keywords

Defaults	None

Examples	> config wps shun-list re-sync

Related Commands	show wps shun-list

config wps signature

To enable or disable Intrusion Detection System (IDS) signature processing, or to enable or disable a specific IDS signature, use the **config wps signature** command.

config wps signature {enable | disable}

config wps signature {standard | custom} state *signature_id* {enable | disable}

Syntax Description

enable disable	Enables or disables IDS signature processing or a specific IDS signature.
standard custom	Configures a standard or custom IDS signature.
state	Specifies the state of the IDS signature.
<i>signature_id</i>	Specifies the identifier for the signature to be enabled or disabled.

Command Default

IDS signature processing is enabled by default.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples

To enable IDS signature processing, which enables the processing of all IDS signatures, enter this command:

```
> config wps signature enable
```

To disable a standard individual IDS signature, enter this command:

```
> config wps signature standard state 15 disable
```

Related Commands

[config wps signature frequency](#)
[config wps signature interval](#)
[config wps signature mac-frequency](#)
[config wps signature quiet-time](#)
[config wps signature reset](#)
[show wps signature events](#)
[show wps signature summary](#)
[show wps summary](#)

config wps signature frequency

To specify the number of matching packets per interval that must be identified at the individual access point level before an attack is detected, use the **config wps signature frequency** command.

config wps signature frequency *signature_id frequency*

Syntax Description	frequency	Sets the frequency of the Intrusion Detection System (IDS) signature.
	<i>signature_id</i>	Specifies the identifier for the signature to be configured.
	<i>frequency</i>	Sets the number of matching packets per interval that must be at the individual access point level before an attack is detected. Range: 1 to 32,000 packets per interval.

Command Default The *frequency* default value varies per signature.

Usage Guidelines If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples To set the number of matching packets per interval per access point before an attack is detected to 1800 for signature ID 4, enter this command:

```
> config wps signature frequency 4 1800
```

Related Commands

- config wps signature
- config wps signature interval
- config wps signature mac-frequency
- config wps signature quiet-time
- config wps signature reset
- show wps signature events
- show wps signature summary
- show wps summary

config wps signature interval

To specify the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval, use the **config wps signature interval** command.

config wps signature interval *signature_id interval*

Syntax Description

interval	Sets the interval of the Intrusion Detection System (IDS) signature.
<i>signature_id</i>	Specifies the identifier for the signature to be configured
<i>interval</i>	Sets the number of seconds that must elapse before the signature frequency threshold is reached. Range: 1 to 3,600 seconds.

Command Default

The default value of *interval* varies per signature.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples

To set the number of seconds to elapse before reaching the signature frequency threshold to 200 for signature ID 1, enter this command:

```
> config wps signature interval 1 200
```

Related Commands

[config wps signature](#)
[config wps signature frequency](#)
[config wps signature mac-frequency](#)
[config wps signature quiet-time](#)
[config wps signature reset](#)
[show wps signature events](#)
[show wps signature summary](#)
[show wps summary](#)

config wps signature mac-frequency

To specify the number of matching packets per interval that must be identified per client per access point before an attack is detected, use the **config wps signature mac-frequency** command.

config wps signature mac-frequency *signature_id* *mac_frequency*

Syntax Description

mac-frequency	Sets the MAC frequency of the Intrusion Detection System (IDS) signature.
<i>signature_id</i>	Specifies the identifier for the signature to be configured.
<i>mac_frequency</i>	Sets the number of matching packets per interval that must be identified per client per access point before an attack is detected. Range: 1 to 32,000 packets per interval.

Command Default

The *mac_frequency* default value varies per signature.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples

To set the number of matching packets per interval per client before an attack is detected to 50 for signature ID 3, enter this command:

```
> config wps signature mac-frequency 3 50
```

Related Commands

[config wps signature](#)
[config wps signature frequency](#)
[config wps signature interval](#)
[config wps signature quiet-time](#)
[config wps signature reset](#)
[show wps signature events](#)
[show wps signature summary](#)
[show wps summary](#)

config wps signature quiet-time

To specify the length of time after which no attacks have been detected at the individual access point level and the alarm can stop, use the **config wps signature quiet-time** command.

config wps signature quiet-time *signature_id* *quiet_time*

Syntax Description

quiet-time	Sets the quiet time of the Intrusion Detection System (IDS) signature.
<i>signature_id</i>	Specifies the identifier for the signature to be configured.
<i>quiet_time</i>	Sets the length of time after which no attacks have been detected at the individual access point level and the alarm can stop. Range: 60 to 32,000 seconds.

Command Default

The default value of *quiet_time* varies per signature.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples

To set the number of seconds after which no attacks have been detected per access point to 60 for signature ID 1, enter this command:

```
> config wps signature quiet-time 1 60
```

Related Commands

[config wps signature](#)
[config wps signature frequency](#)
[config wps signature interval](#)
[config wps signature mac-frequency](#)
[config wps signature reset](#)
[show wps signature events](#)
[show wps signature summary](#)
[show wps summary](#)

config wps signature reset

To reset a specific Intrusion Detection System (IDS) signature or all IDS signatures to default values, use the **config wps signature reset** command.

config wps signature reset {*signature_id* | **all**}

Syntax Description

reset	Resets the IDS signature.
<i>signature_id</i>	Specifies the identifier for the specific IDS signature to be reset.
all	Resets all IDS signatures.

Command Default

config wps signature reset all

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples

To reset the IDS signature 1 to default values, enter this command:

```
> config wps signature reset 1
```

Related Commands

[config wps signature](#)
[config wps signature frequency](#)
[config wps signature interval](#)
[config wps signature mac-frequency](#)
[config wps signature quiet-time](#)
[show wps signature events](#)
[show wps signature summary](#)
[show wps summary](#)

lwapp ap controller ip address

To configure the controller IP address into the H-REAP access point from the access point’s console port, use the **lwapp ap controller ip address** command.

lwapp ap controller ip address *ip_address*

Syntax Description	<i>ip_address</i>	Specifies the IP address of the controller.

Defaults	None.

Usage Guidelines	This command must be entered from an access point’s console port. Prior to changing the H-REAP 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 using the clear lwapp private-config command.



Note

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

Examples	<pre>AP# clear lwapp private-config removing the reap config file flash:/lwapp_reap.cfg AP# lwapp ap controller ip address 10.92.109.1</pre>

Related Commands	<pre>clear lwapp private-config debug lwapp console cli</pre>

Saving Configurations

Use the **save config** command before you log out of the command line interface to save all previous configuration changes.

save config

To save Cisco Wireless LAN controller configurations, use the **save config** command.

save config

Syntax	Description
save	Save switch configurations.
config	Save current settings to NVRAM.

Defaults None.

Examples

```
> save config

Are you sure you want to save? (y/n) y

Configuration Saved!
```

Related Commands `show sysinfo`

Clearing Configurations, Logfiles, and Other Actions

To clear existing configurations, log files, and other functions, use the clear commands.

clear acl counters

To clear the current counters for an access control list (ACL), use the **clear acl counters** command.

clear acl counters *acl_name*

Syntax Description	clear acl	Command action.
	counters	The number of packets hitting the ACLs configured on your controller.
	<i>acl_name</i>	The name of the ACL.

Defaults

None.

Usage Guidelines		
	Note	ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

Examples

> **clear acl counters acl1**

Related Commands

config acl counter
show acl detailed

clear ap-config

Use the **clear ap-config** command to clear (reset to factory default values) a lightweight access point's configuration settings.

clear ap-config *ap_name*

Syntax Description

ap_name	Specifies the access point name.

Defaults

None.

Examples

```
> 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

clear	Delete command.
ap-eventlog	Specifies the state of one or more access point event logs.
specific	Specifies a specific access point log file.
<i>ap_name</i>	Name of access point for which event log file will be emptied.
all	Delete event log for all access points joined to the controller.

Defaults

None.

Examples

```
> 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

Use the **clear ap join stats** commands to clear the join statistics for all access points or for a specific access point.

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

Syntax Description

all	Specifies all access points.
<i>ap_mac</i>	Specifies the access point MAC address.

Defaults

None.

Examples

```
> clear ap join stats all
```

Related Commands

show ap config

clear arp

To clear the ARP table to a Cisco lightweight access point its factory default, use the **clear arp** command.

clear arp

Syntax Description

clear	Clear selected configuration elements.
arp	Clear the ARP table.

Defaults

None.

Examples

```
> clear arp

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

Related Commands

- clear transfer
- clear download filename
- clear download mode
- clear download path
- 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 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	clear	Clear selected configuration elements.
	config	Reset configuration data to factory defaults.
	tsm	Traffic stream metrics.
	802.11a 802.11b	Specifies type of 802.11 network.
	<i>client_mac</i>	Specifies the MAC address of the client.
	<i>ap_mac</i>	MAC address of a Cisco lightweight access point.
	all	All access points.

Defaults	None.

Examples	> 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	clear	Clear selected configuration elements.
	config	Reset configuration data to factory defaults.

Defaults	None.

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

Related Commands	clear transfer
	clear download filename
	clear download mode
	clear download path
	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 ext-webauth-url

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

clear ext-webauth-url

Syntax Description

clear	Clear selected configuration elements.
ext-webauth-url	Clear the external web authentication URL.

Defaults

None.

Examples

```
> clear ext-webauth-url

URL 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 license agent

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

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

Syntax Description	clear	Clear selected configuration elements.
	license agent	License agent settings.
	counters sessions	Counter or session statistics

Defaults	None.

Examples	> clear license agent counters > clear license agent sessions

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

clear	Clear selected configuration elements.
location	Clear location elements.
rfid	Clear Radio Frequency Identification settings.
<i>mac_address</i>	The MAC address of a specific RFID tag.
all	All of the RFID tags in the database.

Defaults

None.

Examples

```
> 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

clear	Clear selected configuration elements.
location	Clear location elements.
statistics	Clear statistics for specified command.
rfid	Clear Radio Frequency Identification settings.

Defaults

None.

Examples

```
> clear location statistics rfid
```

Related Commands

[clear location statistics rfid](#)
[config location](#)
[show location](#)

clear locp statistics

To clear the LOCP statistics, use the **clear locp statistics** command.

clear locp statistics

Syntax Description	clear	Clears selected configuration elements.
	locp statistics	Statistics related to LOCP.

Defaults	None.

Examples	<pre>> clear locp statistics</pre>

Related Commands	clear nmsp statistics config nmsp notify-interval measurement show nmsp notify-interval summary show nmsp statistics show nmsp status

clear login-banner

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

clear login-banner

Syntax Description	clear	Clears selected configuration elements.
	login-banner	Login banner file.

Defaults	None.

Examples	> <code>clear login-banner</code>

Related Commands	transfer download datatype

clear lwapp private-config

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

clear lwapp private-config

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Usage Guidelines	This command is executed from the access point console port. Prior to changing the H-REAP 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 using the clear lwapp private-config command.


Note

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

Examples	<pre>AP# clear lwapp private-config removing the reap config file flash:/lwapp_reap.cfg</pre>

Related Commands	debug capwap debug capwap reap debug lwapp console cli show capwap reap association show capwap reap status

clear nmosp statistics

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

clear nmosp statistics

Syntax Description	clear	Clears selected configuration elements.
	nmosp	Network Mobility Services Protocol settings.
	statistics	Clear NMSP statistics.

Defaults	None.

Examples	To delete the NMSP statistics log file, enter this command: <pre>> clear nmosp statistics</pre>

Related Commands	clear locp statistics config nmosp notify-interval measurement show nmosp notify-interval summary show nmosp 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

<i>index</i>	Specifies the index of the radius accounting server.
all	Specifies all radius accounting servers.

Defaults

None.

Examples

```
> clear radius acct statistics
```

Related Commands

show radius acct statistics

clear radius auth statistics

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

```
clear radius tacacs auth statistics [ index | all ]
```

Syntax Description	<i>index</i>	Specifies the index of the TACACS+ authentication server.
	all	Specifies all TACACS+ authentication servers.

Defaults	None.

Examples	> clear radius 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	clear	Clear selected configuration elements.
	redirect-url	Clear the custom web authentication redirect URL.

Defaults	None.

Examples	<pre>> clear redirect-url URL cleared.</pre>

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	Clear selected configuration elements.

Defaults	None.

Examples	> 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 EAP statistics, use the **clear stats local-auth** command.

clear stats local-auth

Syntax Description

clear	Clear selected configuration elements.
stats	Clear statistics counters.
local-auth	Clear local EAP statistics.

Defaults

None.

Examples

```
> 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	clear	Clear selected configuration elements.
	stats	Clear statistics counters.
	mobility	Clear mobility manager statistics

Defaults	None.

Examples	<pre>> clear stats mobility Mobility stats cleared.</pre>

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

clear	Clear selected configuration elements.
stats	Clear statistics counters.
port	Clear statistics counters for a specific port.
<i>port</i>	Physical interface port number.

Defaults

None.

Examples

```
> 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 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

clear	Clear selected configuration elements.
stats	Clear statistics counters.
radius	Clear statistics regarding radius servers.
{auth acct}	- Clear statistics regarding authentication. - Clear statistics regarding accounting.
{index all}	- The index number of the radius server to be cleared. - Enter all to clear statistics for all radius servers.

Defaults

None.

Examples

```
> clear stats radius auth all
> clear stats radius acct all
> clear stats radius auth 2
```

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 switch

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

clear stats switch

Syntax Description	clear	Clear selected configuration elements.
	stats	Clear statistics counters.
	switch	Clear all switch statistics counters.

Defaults	None.

Examples	<pre>> clear stats switch</pre>

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

Defaults	None.

Examples	> 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

clear	Clear selected configuration elements.
transfer	Clear the transfer information.

Defaults

None.

Examples

```
> 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 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](#)

clear traplog

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

clear traplog

Syntax Description	clear	Clear selected configuration elements.
	traplog	Clear the trap log.

Defaults	None.

Examples	> 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	clear	Clear selected configuration elements.
	webimage	Clear the custom web authentication image.

Defaults	None.

Examples	<pre>> clear webimage</pre>

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	clear	Clear selected configuration elements.
	webmessage	Clear the custom web authentication message.

Defaults	None.

Examples	<pre>> clear webmessage Message cleared.</pre>

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

clear	Clear selected configuration elements.
webtitle	Clear the custom web authentication title.

Defaults

None.

Examples

```
> 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

Uploading and Downloading Files and Configurations

To transfer files to or from the Cisco Wireless LAN controller, use the transfer commands.

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

transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
certpassword	Set a certificate's private key password.
<i>private_key_password</i>	Enter a certificate's private key password or blank to clear the current password.

Defaults

None.

Examples

```
> 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 | webauthcert}

Syntax Description	
transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
datatype	Set download file type.
{config code image login-banner signature webadmincert webauthcert webauthbundle eapdevcert eapcert}	- Enter config to download configuration file. - Enter code to download an executable image to the system. - Enter image to download a web page logo to the system. - Enter login-banner to download a login banner file to the system. - Enter signature to download a signature file to the system. - Enter webadmincert to download a certificate for web administration to the system. - Enter webauthcert to download a web certificate for web portal to the system. - Enter webauthbundle to download custom webauth bundle to the system. - Enter eapdevcert to download an EAP dev certificate to the system. - Enter eapcert to download an EAP ca certificate to the system.

Defaults None.

Examples

```
> transfer download datatype code
```

Related Commands

- clear transfer
- transfer download certpassword
- 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 filename

To download a specific file, use the **transfer download filename** command.

transfer download filename *filename*

Syntax Description	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	filename	Set the FTP or TFTP filename.
	<i>filename</i>	File name up to 512 alphanumeric characters.

Defaults None.

Examples
> **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 filename
- transfer upload mode
- transfer upload path
- transfer upload serverip
- transfer upload start

transfer download mode

To set transfer mode, use the **transfer download mode** command.

transfer download mode {ftp | tftp}

Syntax Description	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	mode	Set transfer mode.
	ftp	Set the transfer mode to ftp.
	tftp	Set the transfer mode to tftp.

Defaults None.

Examples `> transfer download mode tftp`

Related Commands

- clear transfer
- transfer download certpassword
- transfer download filename
- 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 password

To set the password for FTP transfer, use the **transfer download password** command.

transfer download password *password*

Syntax Description	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	password	Set FTP password.
	<i>password</i>	Password.

Defaults	None.

Examples	>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	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	path	Set FTP or TFTP Path.
	<i>path</i>	Directory path.
	Note	Pathnames 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 "/".

Defaults None.

Examples

```
> transfer download path c:\install\version2
```

Related Commands

- clear transfer
- transfer download certpassword
- transfer download filename
- transfer download mode
- 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

transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
port	FTP port.
<i>port</i>	Set FTP port

Defaults

The default FTP *port* is **21**.

Examples

```
>transfer download port 23
```

Related Commands

[transfer download mode](#)
[transfer download password](#)
[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	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	serverip	Enter IP address of the server.
	<i>TFTP_server</i>	TFTP IP address.
	<i>ip_address</i>	Server IP address.

Defaults None.

Examples

```
> transfer download serverip 175.34.56.78
```

Related Commands

- clear transfer
- transfer download certpassword
- transfer download filename
- transfer download mode
- transfer download path
- 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	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	start	Initiate a download.

Defaults None.

Examples

```
> 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 certpassword
- transfer download filename
- transfer download mode
- transfer download path
- transfer download serverip
- 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	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	tftpPktTimeout	Enter the tftp packet timeout.
	<i>timeout</i>	Timeout in seconds between 1 and 254.

Defaults None.

Examples
 > **transfer download tftpPktTimeout 55**

Related Commands

- clear transfer
- transfer download certpassword
- 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

transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
tftpMaxRetries	Enter the number of allowed TFTP packet retries.
<i>retries</i>	Number of allowed TFTP packet retries between 1 and 254 seconds.

Defaults

None.

Examples

```
> transfer download tftpMaxRetries 55
```

Related Commands

clear transfer
transfer download certpassword
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	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	username	FTP port.
	<i>username</i>	Set FTP port.

Defaults	None.

Examples	<pre>>transfer download username ftp_username</pre>

Related Commands	transfer download mode transfer download password transfer download port

transfer encrypt

To configure encryption for config file transfers, use the **transfer encrypt** command.

```
transfer encrypt {enable | disable | set-key key}
```

Syntax Description	transfer	Transfer settings.
	encrypt	Encryption settings.
	enable disable 	Enable or disable this command.
	set-key	Configures the encryption key for configuration file transfers.
	<i>key</i>	Encryption key for config file transfers.

Defaults	None.

Examples	> transfer encrypt enable

Related Commands	clear transfer transfer download datatype transfer download filename transfer download mode transfer download path transfer download serverip transfer upload datatype transfer download filename transfer download mode transfer download path transfer download serverip transfer download 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		
transfer		Transfer settings.
upload		Upload settings.
datatype		Specify data type to upload.
config		Upload the system configuration file.
coredump		Upload the coredump file.
crashfile		Upload the system crash file.
errorlog		Upload the system error log file.
invalid-config		Upload the system invalid-config file.
pac		Upload a Protected Access Credential (PAC).
packet-capture		Upload a packet capture file.
panic-crash-file		Upload the kernel panic information file.
radio-core-dump		Upload the system error log.
signature		Upload the system signature file.
systemtrace		Upload the system trace file.
traplog		Upload the system trap log.
watchdog-crash-file		Upload a console dump file resulting from a software-watchdog-initiated controller reboot following a crash.

Defaults None.

Examples

```
> 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

transfer	Transfer a file to or from the switch.
upload	Transfer a file from the switch.
filename	Set the FTP or TFTP filename.
<i>filename</i>	File name up to 16 alphanumeric characters.

Defaults

None.

Examples

```
> 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}

Syntax Description	transfer	Transfer a file to or from the switch.
	upload	Transfer a file from the switch.
	mode	Set transfer mode.
	ftp	Set the transfer mode to FTP.
	tftp	Set the transfer mode to TFTP.

Defaults	None.

Examples	<pre>> transfer upload mode tftp</pre>

Related Commands	clear transfer transfer upload datatype transfer upload filename 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. The client upload process uses a TFTP or FTP server.

transfer upload pac *username validity password*

Syntax Description	<i>username</i>	Specifies the user identity of the PAC.
	<i>validity</i>	Specifies the validity period(days) of the PAC.
	<i>password</i>	Specifies the password to protect the PAC.

Defaults None.

Examples

```
> transfer upload datatype pac
> transfer upload pac user1 53 pass01
> transfer upload filename uploaded.pac
> transfer upload start
Mode ..... TFTP
TFTP Server IP ..... 10.0.24.21
TFTP Server Path ..... /client/
TFTP Filename ..... uploaded.pac
Data Type ..... PAC
PAC User ..... user1
PAC Validity ..... 53 days
PAC Password ..... pass01
Are you sure you want to start ? (Y/N) y
PAC transfer starting.
File transfer operation completed successfully.
```

Related Commands

[clear transfer](#)
[transfer upload datatype](#)
[transfer upload filename](#)
[transfer upload mode](#)
[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.

transfer upload password *password*

Syntax Description	transfer	Transfer a file to or from the controller.
	upload	Transfer a file from the controller.
	password	Set FTP server password.
	<i>password</i>	Specify the password needed to access the FTP server..

Defaults None.

Examples

```
>transfer upload password pass01
```

Related Commands

- [clear transfer](#)
- [transfer upload datatype](#)
- [transfer upload filename](#)
- [transfer upload mode](#)
- [transfer upload pac](#)
- [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	transfer	Transfer a file to or from the switch.
	upload	Transfer a file from the switch.
	path	Set TFTP or FTP Path.
	<i>path</i>	Server path to file.

Defaults None.

Examples

```
> transfer upload path c:\install\version2
```

Related Commands

- [clear transfer](#)
- [transfer upload datatype](#)
- [transfer upload filename](#)
- [transfer upload mode](#)
- [transfer upload pac](#)
- [transfer upload password](#)
- [transfer upload port](#)
- [transfer upload serverip](#)
- [transfer upload start](#)
- [transfer upload username](#)

transfer upload port

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

transfer upload port *port*

Syntax Description	transfer	Transfer a file to or from the switch.
	upload	Transfer a file from the switch.
	port	FTP port.
	<i>port</i>	Set FTP port.

Defaults The default FTP port is **21**.

Examples

```
>transfer upload port 23
```

Related Commands

- [clear transfer](#)
- [transfer upload datatype](#)
- [transfer upload filename](#)
- [transfer upload mode](#)
- [transfer upload pac](#)
- [transfer upload password](#)
- [transfer upload path](#)
- [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	transfer	Transfer a file to or from the switch.
	upload	Transfer a file from the switch.
	serverip	Enter IP address of the server.
	<i>ip_address</i>	Server IP address.

Defaults None.

Examples > **transfer upload serverip 175.34.56.78**

Related Commands

- [clear transfer](#)
- [transfer upload datatype](#)
- [transfer upload filename](#)
- [transfer upload mode](#)
- [transfer upload pac](#)
- [transfer upload password](#)
- [transfer upload path](#)
- [transfer upload port](#)
- [transfer upload start](#)
- [transfer upload username](#)

transfer upload start

To initiate an upload, use the **transfer upload start** command.

transfer upload start

Syntax Description	transfer	Transfer a file to or from the switch.
	upload	Transfer a file from the switch.
	start	Initiate upload.

Defaults None.

Examples

```
> 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 datatype](#)
- [transfer upload filename](#)
- [transfer upload mode](#)
- [transfer upload pac](#)
- [transfer upload password](#)
- [transfer upload path](#)
- [transfer upload port](#)
- [transfer upload serverip](#)
- [transfer upload username](#)

transfer upload username

To specify the FTP username, use the **transfer upload username** command.

transfer download username *username*

Syntax Description	transfer	File transfer settings.
	upload	Transfer a file from the controller.
	username	Specify the FTP server username.
	<i>username</i>	The user name required to access the FTP server.

Defaults None.

Examples `>transfer upload username ftp_username`

Related Commands

- [clear transfer](#)
- [transfer upload datatype](#)
- [transfer upload filename](#)
- [transfer upload mode](#)
- [transfer upload pac](#)
- [transfer upload password](#)
- [transfer upload path](#)
- [transfer upload port](#)
- [transfer upload serverip](#)
- [transfer upload start](#)

Installing and Modifying Licenses

Use the **license** commands to install, remove, modify, or rehost licenses.



Note

The **license** commands are available only on the Cisco 5500 series controller.



Note

For detailed information on installing and rehosting licenses on the Cisco 5500 series controller, refer to the “Installing and Configuring Licenses” section in chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide*.

license clear

To remove a license from the Cisco 5500 series controller, use the **license clear** command.

license clear *license_name*

Syntax Description	license	License settings.
	clear	Install settings.
	<i>license_name</i>	Name of the license.

Defaults 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

```
> 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

license	License settings.
comment	Comment settings.
add delete	Add or delete a comment.
<i>license_name</i>	Name of the license.
<i>comment_string</i>	License comment.

Defaults

None

Examples

```
> 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	license	License settings.
	install	Install settings.
	<i>url</i>	The URL of the TFTP server (tftp://server_ip/path/filename).

Defaults	None

Usage Guidelines	Cisco recommends 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	> license install tftp://10.10.10.10/path/license.lic

Related Commands	license clear license modify priority 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

license	License settings.
modify priority	Modify priority setting.
<i>license_name</i>	Name of the ap-count evaluation license.
high low	Modify the priority of an ap-count evaluation license.

Defaults

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, thereby forcing 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

```
> license modify priority wplus-ap-count high
```

Related Commands

[license clear](#)
[license install](#)
[license revoke](#)
[license save](#)
[show license all](#)

license revoke

Revoking a license from one controller and installing it on another is called *rehosting*. You might want to rehost a license in order to change the purpose of a controller. For example, if you want to move your OfficeExtend or indoor mesh access points to a different controller, you could transfer the wplus license from one controller to another.

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

license	License settings.
revoke	Revoke license settings.
<i>permission_ticket_url</i>	The URL of the TFTP server (tftp://server_ip/path/filename) where you saved the permission ticket.
rehost	Rehost license settings.
<i>rehost_ticket_url</i>	The URL of the TFTP server (tftp://server_ip/path/filename) where you saved the rehost ticket.

Defaults

None.

Usage Guidelines

Before you revoke a license, save the device credentials 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, refer to the “Installing and Configuring Licenses” section in chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide*.

Examples

```
license revoke tftp://10.10.10.10/path/permit_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

license	License settings.
save	Save settings.
credential	Save device credential information to a file.
<i>url</i>	The URL of the TFTP server (tftp://server_ip/path/filename).

Defaults

None.

Usage Guidelines

Save the device credentials before you revoke the license (using the **license revoke** command).

Examples

```
>license save credential tftp://10.10.10.10/path/cred.lic
```

Related Commands

[license clear](#)
[license install](#)
[license modify priority](#)
[license revoke](#)
[show license all](#)

Troubleshooting Commands

Use the **debug** commands to manage system debugging.



Caution

Debug commands are reserved for use only under direction of Cisco personnel. Please do not use these commands without direction from Cisco-certified staff.



Note

Enabling all **debug** commands on a system with many clients authenticating may result in some debugs being lost.

debug aaa

To configure AAA debug options, use the **debug aaa** command:

```
debug aaa {[all | detail | events | packet | ldap | local-auth | tacacs] [enable | disable]}
```

Syntax Description

all	Specifies debugging of all AAA messages.
detail	Specifies debugging of AAA errors.
events	Specifies debugging of AAA events.
packet	Specifies debugging of AAA packets.
ldap	Specifies debugging of the AAA LDAP events.
local-auth	Specifies debugging of the AAA local EAP events.
tacacs	Specifies debugging of the AAA TACACS+ events.
enable	Starts the debugging feature.
disable	Stops the debugging feature.

Defaults

None.

Examples

```
> debug aaa ldap enable
```

Related Commands

```
debug aaa local-auth eap  
show running-config
```


debug aaa local-auth

To debug AAA local authentication on the controller, use the **debug aaa local-auth** command:

```
debug aaa local-auth { db | shim | eap { framework | method } { all | errors | events | packets | sm } }
                    { enable | disable }
```

Syntax Description		
db		Configures debugging of the AAA local authentication backend messages and events.
shim		Configures debugging of the AAA local authentication shim layer events.
eap		Configures debugging of the AAA local EAP authentication.
framework		Configures debugging of the local EAP framework.
method		Configures debugging of local EAP methods.
all		Specifies debugging of local EAP messages.
errors		Specifies debugging of local EAP errors.
events		Specifies debugging of local EAP events.
packets		Specifies debugging of local EAP packets.
sm		Specifies debugging of the local EAP state machine.
enable disable		Start or stop the debugging feature.

Defaults None.

Examples

```
> debug aaa local-auth eap method all enable
```

Related Commands

- [clear stats local-auth](#)
- [config local-auth active-timeout](#)
- [config local-auth eap-profile](#)
- [config local-auth method fast](#)
- [config local-auth user-credentials](#)
- [show local-auth certificates](#)
- [show local-auth config](#)
- [show local-auth statistics](#)

debug airewave-director

To configure the Airewave Director Software debug options, use the **debug airewave-director** command.

debug airewave-director { **all** | **channel** | **detail** | **error** | **group** | **manager** | **message** | **packet** | **power** | **profile** | **radar** | **rf-change** } { **enable** | **disable** }

Syntax Description

debug	Diagnostic and troubleshooting parameters.
airewave-director	Airewave Director parameters.
all channel detail error group manager message packet power profile radar rf-change	- Enter all to configure debug of all Airewave Director logs. - Enter channel to configure debug of Airewave Director channel assignment protocol - Enter detail to configure debug of Airewave Director detail logs. - Enter error to configure debug of Airewave Director error logs. - Enter group to configure debug of Airewave Director grouping protocol. - Enter manager to configure debug of Airewave Director manager. - Enter message to configure debug of Airewave Director messages. - Enter packet to configure debug of Airewave Director packets. - Enter power to configure debug of Airewave Director power assignment protocol and coverage hole detection. - Enter profile to configure debug of Airewave Director profile events. - Enter radar to configure debug of Airewave Director radar detection/avoidance protocol. - Enter rf-change to configure debug of Airewave Director rf changes.
enable disable	- Enter enable to enable Airewave Director debug setting. - Enter disable to disable Airewave Director debug setting.

Defaults

None.

Examples

```
> debug airewave-director profile enable
> debug airewave-director profile disable
```

Related Commands

show sysinfo
debug disable-all

debug ap

To enable or disable remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use this command:

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

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

Defaults

Disabled.

Examples

To enable remote debugging on access point AP01:

```
> debug ap enable AP01
```

To execute the **config ap location** command on access point AP02:

```
> debug ap command "config ap location "Building 1" AP02"
```

To execute the flash LED command on access point AP03:

```
> debug ap command "led flash 30" AP03
```

Related Commands

```
show sysinfo
config sysname
```

debug ap enable

To enable or disable remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use this command:

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

Syntax Description

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

Defaults

None.

Examples

To enable remote debugging on access point AP01:

```
> debug ap enable AP01
```

To disable remote debugging on access point AP02:

```
> debug ap disable AP02
```

To execute the flash LED command on access point AP03:

```
> debug ap command "led flash 30" AP03
```

Related Commands

show sysinfo
config sysname

debug arp

To configure ARP debug options, use the **debug arp** command.

debug arp {all | detail | events | message} {enable | disable}

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	arp	ARP parameters.
	all detail error message	- Enter all to configure debug of all arp logs. - Enter detail to configure debug of arp detail messages.. - Enter error to configure debug of arp errors. - Enter message to configure debug of arp messages.
	enable disable	- Enter enable to enable arp debug setting. - Enter disable to disable arp debug setting.

Defaults None.

Examples

```
> debug arp error enable
> debug arp error disable
```

Related Commands

```
show sysinfo
debug disable-all
```

debug bcast

To configure debug of broadcast options, use the **debug bcast** command.

```
debug bcast {all | error | message | igmp | detail} {enable | disable}
```

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	bcast	bcast parameters.
	all error message igmp detail	- Enter all to configure debug of all broadcast logs. - Enter detail to configure debug of broadcast detailed messages. - Enter error to configure debug of broadcast errors. - Enter igmp to configure debug of broadcast messages. - Enter message to configure debug of broadcast messages.
	enable disable	- Enter enable to enable broadcast debug setting. - Enter disable to disable broadcast debug setting.

Defaults None.

Examples > debug bcast message enable
> debug bcast message disable

Related Commands show sysinfo
 debug disable-all

debug cac

To configure call admission control (CAC) debug options, use the **debug cac** command.

debug cac {all | event | packet} {enable | disable}

Syntax Description	debug	Diagnostic and troubleshooting settings.
	cac	Debug call admission control settings.
	all event packet	- Enter all to configure debugging options for all CAC messages. - Enter event to configure debugging options for CAC events. - Enter packet to configure debugging options for selected CAC packets.
	enable disable	- Enter enable to enable debug setting. - Enter disable to disable debug setting.

Defaults Disabled.

Examples

```
> debug cac event enable
> debug cac event disable
```

Related Commands

```
config 802.11 cac video acm
config 802.11 {enable | disable} network
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 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 stream-size
config 802.11 cac voice tspec-inactivity-timeout
```

debug capwap

To obtain troubleshooting information about Control and Provisioning of Wireless Access Points (CAPWAP) settings, use the **debug capwap** command.

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

Syntax Description	debug	Diagnostic and troubleshooting settings.
	capwap	Control and Provisioning of Wireless Access Points settings
	detail	Debug CAPWAP detail settings.
	dtls-keepalive	Debug CAPWAP DTLS data keepalive packets settings.
	errors	Debug CAPWAP error settings.
	events	Debug CAPWAP events settings.
	hexdump	Debug CAPWAP hexadecimal dump settings.
	info	Debug CAPWAP info settings.
	packet	Debug CAPWAP packet settings.
	payload	Debug CAPWAP payload settings.
	enable disable	Enable or disable this command.

Command Default	None.

Examples	> debug capwap detail enable

Related Commands	clear lwapp private-config debug disable-all show capwap reap association show capwap reap status

debug capwap reap

To obtain troubleshooting information about Control and Provisioning of Wireless Access Points (CAPWAP) settings on a Hybrid Remote Edge Access Point (hybrid-REAP) access point, use the **debug capwap reap** command.

debug capwap reap [mgmt | load]

Syntax Description	debug	Diagnostic and troubleshooting settings.
	capwap	Control and Provisioning of Wireless Access Points settings.
	reap	Debug hybrid-REAP settings.
	mgmt	(Optional) Debug client authentication and association messages.
	load	(Optional) Display payload activities, which is useful when the hybrid-REAP access point boots up in standalone mode..

Command Default	None.

Examples	To do this, enter this command: > example

Related Commands	clear lwapp private-config debug disable-all show capwap reap association show capwap reap status

debug crypto

To configure hardware cryptographic debug options, use the **debug crypto** command.

```
debug crypto {all | sessions | trace | warning} {enable | disable}
```

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	dhcp	DHCP parameters.
	all sessions trace warning	- Enter all to configure debug of all hardware crypto messages. - Enter sessions to configure debug of hardware crypto sessions. - Enter trace to configure debug of hardware crypto sessions. - Enter warning to configure debug of hardware crypto sessions.
	enable disable	- Enter enable to enable debug setting. - Enter disable to disable debug setting.

Defaults
None.

Examples

```
> debug sessions enable
> debug sessions disable
```

Related Commands

show sysinfo

debug disable-all

debug dhcp

To configure DHCP debug options, use the **debug dhcp** command.

debug dhcp {message | packet} {enable | disable}

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	dhcp	DHCP parameters.
	message packet	- Enter message to configure debug of DHCP error messages. - Enter packet to configure debug of DHCP packets.
	enable disable	- Enter enable to enable DHCP debug setting. - Enter disable to disable DHCP debug setting.

Defaults None.

Examples

```
> debug dhcp message enable
> debug dhcp message disable
```

Related Commands

- [config dhcp](#)
- [config dhcp proxy](#)
- [config interface dhcp](#)
- [config wlan dhcp_server](#)
- [debug dhcp service-port](#)
- [debug disable-all](#)
- [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	debug	Diagnostic and troubleshooting parameters.
	dhcp	DHCP parameters.
	service-port	Debug service Port settings.
	enable disable	Enable or disable this command.

Command Default	None

Examples	To enable debugging of DHCP packets on a service port, enter the following command: > debug dhcp service-port enable

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

debug disable-all

To disable all debug messages, use the **debug disable-all** command.

debug disable-all

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	disable-all	Disables all debug messages.

Defaults	Disabled.

Examples	> debug disable-all

Related Commands	None.

debug dot11

To configure dot11 events debug options, use the **debug dot11** command.

```
debug dot11 {all | load-balancing | management | mobile | rfid | rldp | rogue | state} {enable | disable}
```

Syntax Description

debug	Diagnostic and troubleshooting parameters.
dot11	dot11 events parameters.
all load-balancing management mobile rfid rldp rogue state	- Enter all to configure debug of all 802.11 messages. - Enter load-balancing to configure debug of 802.11 load balancing events. - Enter management to configure debug of 802.11 MAC management messages. - Enter mobile to configure debug of 802.11 mobile events. - Enter rfid to configure debug of 802.11 RFID tag module. - Enter rldp to configure debug of 802.11 Rogue Location Discovery. - Enter rogue to configure debug of 802.11 rogue events. - Enter state to configure debug of 802.11 mobile state transitions.
enable disable	- Enter enable to enable dot11 debug setting. - Enter disable to disable dot11 debug setting.

Defaults

None.

Examples

```
> debug dot11 state enable
> debug dot11 state disable
```

Related Commands

```
debug disable-all
debug dot11 mgmt interface
debug dot11 mgmt msg
debug dot11 mgmt ssid
debug dot11 mgmt state-machine
debug dot11 mgmt station
```

debug dot11 mgmt interface

To view 802.11 management interface events, use the **debug dot11 mgmt interface** command.

debug dot11 mgmt interface

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	<pre>> debug dot11 mgmt interface</pre>

Related Commands	debug disable-all debug dot11 debug dot11 mgmt msg debug dot11 mgmt ssid debug dot11 mgmt state-machine debug dot11 mgmt station

debug dot11 mgmt msg

To view 802.11 management messages, use the **debug dot11 mgmt msg** command.

debug dot11 mgmt msg

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	> <code>debug dot11 mgmt msg</code>

Related Commands	debug disable-all debug dot11 debug dot11 mgmt interface debug dot11 mgmt ssid debug dot11 mgmt state-machine debug dot11 mgmt station

debug dot11 mgmt ssid

To view 802.11 SSID management events, use the **debug dot11 mgmt ssid** command.

debug dot11 mgmt ssid

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	<pre>> debug dot11 mgmt ssid</pre>

Related Commands	debug disable-all debug dot11 debug dot11 mgmt interface debug dot11 mgmt msg debug dot11 mgmt state-machine debug dot11 mgmt station

debug dot11 mgmt state-machine

To view 802.11 state machine, use the **debug dot11 mgmt state-machine** command.

debug dot11 mgmt state-machine

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	<pre>> debug dot11 mgmt state-machine</pre>

Related Commands	debug disable-all debug dot11 debug dot11 mgmt interface debug dot11 mgmt msg debug dot11 mgmt ssid debug dot11 mgmt station

debug dot11 mgmt station

To view client events, use the **debug dot11 mgmt station** command.

debug dot11 mgmt station

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	<pre>> debug dot11 mgmt station</pre>

Related Commands	debug disable-all debug dot11 debug dot11 mgmt interface debug dot11 mgmt msg debug dot11 mgmt ssid debug dot11 mgmt state-machine

debug dot1x

To configure dot1x debug options, use the **debug dot1x** command.

```
debug dot1x {aaa | all | events | packet | states} {enable | disable}
```

Syntax Description	debug	Diagnostic and troubleshooting settings.
	dot1x	dot1x settings.
	aaa all events packet states	- Enter aaa to configure debug of 802.1X AAA interactions. - Enter all to configure debug of all 802.1x messages. - Enter events to configure debug of 802.1x 802.1X events. - Enter packet to configure debug of 802.1x 802.1X packets. - Enter states to configure debug of 802.1x mobile state transitions.
	enable disable	- Enter enable to enable dot1x debug setting. - Enter disable to disable dot1x debug setting.

Defaults
None.

Examples
To enable debugging of dot1x mobile state transitions, enter the following command:

```
> debug dot1x state enable
```

To disable debugging of all dot1x interactions, enter the following command:

```
> debug dot1x all disable
```

Related Commands

- debug disable-all
- debug dot11
- debug dot11 mgmt interface
- debug dot11 mgmt msg
- debug dot11 mgmt ssid
- debug dot11 mgmt state-machine
- debug dot11 mgmt station

debug group

To enable or disable troubleshooting of access point groups, use the **debug group** command.

debug group {enable | disable}

Syntax Description	debug	Diagnostic and troubleshooting settings.
	group	Access point group settings.
	enable disable	- Enter enable to enable access point group debugging. - Enter disable to disable access point group debugging.

Defaults	None.

Examples	To enable debugging of access point groups, enter the following command: <pre>> debug group enable</pre>

Related Commands	config guest-lan nac config wlan apgroup config wlan nac

debug hreap aaa

To enable or disable debugging of hybrid-REAP (HREAP) backup RADIUS server events or errors, use the **debug hreap aaa** command.

debug hreap aaa {event | error} {enable | disable}

Syntax Description

debug	Diagnostic and troubleshooting parameters.
hreap	HREAP parameters.
aaa	Authentication server parameters.
event	Enter event to debug HREAP RADIUS server events.
error	Enter error to debug HREAP RADIUS server errors.
enable disable	Enable or disable this command.

Command Default

None.

Examples

To enable debugging of HREAP RADIUS server events, enter the following command:

```
> debug hreap aaa event enable
```

Related Commands

[debug disable-all](#)
[debug hreap cckm](#)
[debug hreap group](#)
[config hreap group](#)
[show hreap group detail](#)
[show hreap group summary](#)
[show radius summary](#)

debug hreap cckm

To enable or disable debugging of hybrid-REAP (HREAP) Cisco Centralized Key Management (CCKM fast roaming), use the **debug hreap cckm** command.

debug hreap cckm {enable | disable}

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	hreap	HREAP parameters.
	cckm	CCKM fast roaming parameters.
	enable disable	Enable or disable this command.

Command Default None.

Examples To enable debugging of HREAP CCKM fast roaming events, enter the following command:
> **debug hreap cckm event enable**

Related Commands

- [debug disable-all](#)
- [debug hreap aaa](#)
- [debug hreap group](#)
- [config hreap group](#)
- [show hreap group detail](#)
- [show hreap group summary](#)
- [show radius summary](#)

debug hreap group

To enable or disable debugging of hybrid-REAP (HREAP) access point groups, use the **debug hreap group** command.

```
debug hreap group {enable | disable}
```

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	hreap	Hybrid Remote Edge Access Point parameters.
	group	HREAP access point group parameters.
	enable disable	Enable or disable this command.

Command Default None.

Examples To enable debugging of HREAP access point groups, enter the following command:
> debug hreap cckm event enable

Related Commands [debug disable-all](#)
[debug hreap aaa](#)
[debug hreap cckm](#)
[config hreap group](#)
[show hreap group detail](#)
[show hreap group summary](#)

debug l2age

To configure debug of Layer 2 Age timeout messages, use the **debug l2age** command.

debug l2age {enable | disable}

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	l2age	Layer 2 Age Timeout Messages.
	enable disable	- Enter enable to enable l2age debug setting. - Enter disable to disable l2age debug setting.

Defaults	None.

Examples	<pre>> debug l2age enable > debug l2age disable</pre>

Related Commands	debug disable-all

debug lwapp console cli

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

debug lwapp console cli



Note

This access point CLI command must be issued from the access point console port.

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Examples

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

Related Commands

[debug disable-all](#)
[debug ap](#)
[clear lwapp private-config](#)

debug mac

To configure MAC address debugging, use the **debug mac** command.

debug mac {**disable** | **addr** *MAC*}

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	mac	MAC address parameters.
	disable	Enter disable to disable MAC debugging.
	addr	Enter addr to configure the MAC address.
	<i>MAC</i>	MAC address.

Defaults	None.

Examples	> debug mac addr 00.oc.41.07.33.a6 > debug mac disable

Related Commands	debug disable-all

debug memory

To enable or disable debugging of errors or events during controller memory allocation, use this command:

```
debug memory {errors | events} {enable | disable}
```

Syntax Description

debug	Diagnostic and troubleshooting settings.
memory	Cisco Wireless LAN Controller memory settings.
errors	Troubleshoot memory leak errors.
events	Troubleshoot memory leak events.
enable disable	Enable or disable this command.

Command Default

Disabled.

Examples

```
> debug memory events enable
```

Related Commands

[config memory monitor errors](#)
[config memory monitor leaks](#)
[show memory monitor](#)

debug mesh security

To begin debugging mesh security problems, use the **debug mesh security** command.

debug mesh security {all | events | errors} {enable | disable}

Syntax Description	debug	Diagnostic and troubleshooting settings.
	mesh	Troubleshoot mesh access point problems.
	security	Troubleshoot mesh security problems.
	all events errors	- Enter all to debug all mesh security messages. - Enter events to debug mesh security event messages. - Enter errors to debug mesh security error messages.
	enable disable	Enable or disable this command.

Defaults This command has no defaults.

Examples > **debug mesh security errors enable**

Related Commands [config mesh security](#)
[show mesh security-stats](#)

debug mobility

To troubleshoot wireless mobility issues, use the **debug mobility** command.

```
debug mobility {{directory | handoff | multicast}{enable | disable} |
keep-alive {enable | disable} {all | IP_address}}
```

Syntax Description

debug	Diagnostic and troubleshooting settings.
mobility	Wireless mobility settings.
directory	Start debugging of wireless mobility error messages.
handoff	Start debugging of wireless mobility packets.
multicast	Start debugging of multicast mobility packets.
keep-alive	Start debugging of wireless mobility keepalive messages.
<i>IP_address</i>	IP address of wireless mobility client.
enable disable	Enable or disable this debugging feature.

Defaults

None.

Examples

```
> debug mobility handoff enable
> debug mobility keep-alive disable all
> debug mobility keep-alive enable 172.19.28.40
> debug mobility multicast enable
```

Related Commands

[config guest-lan mobility 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 mobility statistics reset](#)
[config wlan mobility anchor](#)
[show mobility anchor](#)
[show mobility statistics](#)
[show mobility summary](#)

debug nac

To configure debug of Network Access Control (NAC), use the **debug nac** command.

debug nac {events | packet} {enable | disable}

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	nac	Network Access Control (NAC) parameters.
	events packet	- Enter events to configure debug of NAC events. - Enter packet to configure debug of NAC packets.
	enable disable	- Enter enable to enable NAC debug setting. - Enter disable to disable NAC debug setting.

Defaults	None.

Examples	<pre>> debug nac events enable > debug nac events disable</pre>

Related Commands	show nac statistics show nac summary config guest-lan nac config wlan nac

debug nmosp

To configure debug of Network Mobility Services Protocol (NMSP), use the **debug nmosp** command.

```
debug nmosp {all | connection | detail | error | event | message | packet}
```

Syntax Description	debug	Diagnostic and troubleshooting settings.
	nmosp	Network Mobility Services Protocol settings.
	all	Debug all NMSP messages.
	connection	Debug NMSP connection events.
	detail	Debug NMSP events in detail.
	error	Debug NMSP error messages.
	event	Debug NMSP events.
	message	Debug NMSP transmit and receive messages.
	packet	Debug NMSP packet events.

Defaults None.

Examples > debug nmosp connection
> debug nmosp error

Related Commands [clear nmosp statistics](#)
[debug disable-all](#)
[config nmosp notify-interval measurement](#)

debug ntp

To configure debug of Network Time Protocol (NTP), use the **debug ntp** command.

debug ntp {**detail** | **low** | **packet**} {**enable** | **disable**}

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	ntp	Network Time Protocol (NTP) parameters.
	{ detail low packet }	- Enter detail to configure debug of detailed NTP messages. - Enter low to configure debug of NTP messages. - Enter packet to configure debug of NTP packets.
	{ enable disable }	- Enter enable to enable NTP debug setting. - Enter disable to disable NTP debug setting.

Defaults None.

Examples

```
> debug ntp packet enable
> debug ntp packet disable
```

Related Commands debug disable-all

debug pem

To configure the access policy manager debug options, use the **debug pem** command.

```
debug pem {events | state} {enable | disable}
```

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	pem	Access policy manager debug options.
	{events state}	- Enter packet to configure debug of policy manager events.. - Enter events to configure debug of policy manager State Machine.
	{enable disable}	- Enter enable to enable access policy manager debug setting. - Enter disable to disable access policy manager debug setting.

Defaults None.

Examples

```
> debug pem state enable
> debug pem state disable
```

Related Commands debug disable-all

debug pm

To configure debug of security policy manager module, use the **debug pm** command.

```
debug pm {all disable | {config | hwcrypto | ikemsg | init | list | message | pki | rng | rules |
sa-export | sa-import | ssh-l2tp | ssh-appgw | ssh-engine | ssh-int | ssh-pmgr | ssh-ppp |
ssh-tcp} {enable | disable} }
```

Syntax Description		
debug		Diagnostic and troubleshooting settings.
pm		Security policy manager module settings.
all disable		Used to disable all debugging in the policy manager module.
config hwcrypto ikemsg init list message pki rng rules sa-export sa-import ssh-l2tp ssh-appgw ssh-engine ssh-int ssh-pmgr ssh-ppp ssh-tcp		- Enter config to configure debug of policy manager configuration. - Enter hwcrypto to configure debug of hardware offload events. - Enter ikemsg to configure debug of IKE messages. - Enter init to configure debug of policy manager initialization events. - Enter list to configure debug of policy manager list mgmt. - Enter message to configure debug of policy manager message queue events. - Enter pki to configure debug of PKI-related events. - Enter rng to configure debug of random number generation. - Enter rules to configure debug of layer 3 policy events. - Enter sa-export to configure debug of SA export (mobility). - Enter sa-import to configure debug of SA import (mobility). - Enter ssh-l2tp to configure debug of policy manager l2tp handling. - Enter ssh-appgw to configure debug of application gateways. - Enter ssh-engine to configure debug of the policy manager engine. - Enter ssh-int to configure debug of the policy manager interceptor. - Enter ssh-pmgr to configure debug of the policy manager policy mgr. - Enter ssh-ppp to configure debug of policy manager ppp handling. - Enter ssh-tcp to configure debug of policy manager tcp handling.
enable disable		Enable or disable the designated command.

Defaults None.

Examples

```
> debug pm pki enable
> debug pm ssh-pmgr disable
```

Related Commands [debug disable-all](#)

debug poe

To configure debug of Power over Ethernet debug options, use the **debug poe** command.

```
debug poe {detail | error | message} {enable | disable}
```

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	poe	Power over ethernet debug options parameters.
	detail error message	- Enter detail to configure debug of POE detail logs. - Enter error to configure debug of POE error logs. - Enter message to configure debug of POE messages.
	enable disable	- Enter enable to enable POE debug setting. - Enter disable to disable POE debug setting.

Defaults	None.

Examples	<pre>> debug poe message enable > debug poe message disable</pre>

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	debug	Diagnostic and troubleshooting parameters.
	rbc	RBC parameters.
	{all detail errors packet}	- Enter all to configure debug of RBC. - Enter detail to configure debug of RBC detail. - Enter errors to configure debug of RBC errors. - Enter packet to configure debug of RBC packet trace.
	{enable disable}	- Enter enable to enable RBC debug setting. - Enter disable to disable RBC debug setting.

Defaults	None.

Examples	<pre>> debug rbc packet enable > debug rbc packet disable</pre>

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 | nmosp | receive} {enable | disable}
```

Syntax Description	debug	Diagnostic and troubleshooting settings.
	rbcp	RBCP settings.
	all detail errors nmosp receive	- Enter all to configure debug of all RFID messages. - Enter detail to configure debug of RFID detail. - Enter errors to configure debug of RFID error messages. - Enter nmosp to configure debug of RFID Network Mobility Services Protocol (NMSP) messages. - Enter receive to configure debug of incoming RFID tag messages.
	enable disable	Enable or disable RFID debug setting.

Defaults None.

Examples > debug rfid errors enable
 > debug rfid errors disable

Related Commands [debug disable-all](#)

debug service ap-monitor

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

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

Syntax Description	debug	Diagnostic and troubleshooting settings.
	service	Services settings.
	ap-monitor	Access point monitoring services.
	all	Configure debugging of all access point status messages.
	error	Configure debugging of access point monitor error events.
	event	Configure debugging of access point monitor events.
	nmsp	Configure debugging of access point monitor NMSP events.
	packet	Configure debugging of access point monitor packets.
	enable disable	Enable or disable this command.

Command Default	None.

Examples	To troubleshoot and debug access point monitor NMSP events, use this command: <pre>> debug service ap-monitor events</pre>

Related Commands	debug disable-all show nmsp status

debug snmp

To configure SNMP debug options, use the **debug snmp** command.

```
debug snmp {agent | all | mib | trap} {enable | disable}
```

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	snmp	lwapp parameters.
	{agent all mib trap}	- Enter agent to configure debug of SNMP agent. - Enter all to configure debug of all SNMP messages. - Enter mib to configure debug of SNMP MIB. - Enter trap to configure debug of SNMP traps.
	{enable disable}	- Enter enable to enable SNMP debug setting. - Enter disable to disable SNMP debug setting.

Defaults None.

Examples > debug snmp trap enable
> debug snmp trap disable

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	debug	Diagnostic and troubleshooting parameters.
	transfer	transfer parameters.
	{ all tftp trace }	- Enter all to configure debug of all transfer messages. - Enter tftp to configure debug of tftp transfers. - Enter trace to configure debug of transfer/upgrade.
	{ enable disable }	- Enter enable to enable transfer debug setting. - Enter disable to disable transfer debug setting.

Defaults None.

Examples

```
> debug transfer trace enable
> debug transfer trace disable
```

Related Commands debug disable-all

debug wcp

To configure wcp debug options, use the **debug wcp** command.

```
debug wcp {events | packet} {enable | disable}
```

Syntax Description	debug	Diagnostic and troubleshooting parameters.
	wcp	wcp parameters.
	{events packet}	- Enter events to configure debug of WLAN Control Protocol (WCP) Events. - Enter packet to configure debug of WLAN Control Protocol (WCP) Packets.
	{enable disable}	- Enter enable to enable wcp debug setting. - Enter disable to disable wcp debug setting.

Defaults None.

Examples

```
> debug wcp packet enable
> debug wcp packet disable
```

Related Commands debug disable-all

debug wps sig

To troubleshoot Wireless Provisioning Service (WPS) signature settings, use the **debug wps sig** command.

debug wps sig {enable | disable}

Syntax Description	debug	Diagnostic and troubleshooting settings.
	wps	Wireless Provisioning Service settings.
	sig	Signature settings.
	enable disable	Enable or disable this command

Defaults None.

Examples

```
> debug wps sig enable
> debug wps sig disable
```

Related Commands

[debug disable-all](#)
[debug wps mfp](#)

debug wps mfp

To troubleshoot WPS Management Frame Protection (MFP) settings, use the **debug wps mfp** command.

```
debug wps mfp { client | capwap | detail | report | mm } { enable | disable }
```

Syntax Description	debug	Diagnostic and troubleshooting settings.
	wps	Wireless Provisioning Service settings.
	mfp	Management Frame Protection settings.
	client	Configures debugging for client MFP messages.
	capwap	Configures debugging for MFP messages between the controller and access points.
	detail	Configures detailed debugging for MFP messages.
	report	Configures debugging for MFP reporting.
	mm	Configures debugging for MFP mobility (inter-controller) messages.
	enable disable	Enable or disable this command.

Defaults None.

Examples > debug wps mfp detail enable
 > debug wps mfp mm disable

Related Commands [debug disable-all](#)
 [debug wps sig](#)

eping

To test mobility Ethernet over IP (EoIP) data packet communication between two controllers, use the **eping** command.

eping *mobility_peer_IP_address*

Syntax Description	eping	Initiate a ping request and reply message for EoIP mobility packets.
	<i>mobility_peer_IP_address</i>	The IP address of a controller that belongs to a mobility group.

Defaults	None.

Usage Guidelines	This command tests the mobility data traffic over the management interface.



Note	This ping test is not Internet Control Message Protocol (ICMP) based. The term “ping” is used to indicate an echo request and an echo reply message.

Examples	> eping 172.12.35.31

Related Commands	mping
	config logging buffered debugging
	show logging
	debug mobility handoff enable

mping

To test mobility UDP control packet communication between two controllers, use the **mping** command.

mping *mobility_peer_IP_address*

Syntax Description	mping	Initiate a ping request and reply message for UDP mobility packets.
	<i>mobility_peer_IP_address</i>	The IP address of a controller that belongs to a mobility group.

Defaults	None.

Usage Guidelines	This test runs over mobility UDP port 16666. It tests whether the mobility control packet can be reached over the management interface.



Note This ping test is not Internet Control Message Protocol (ICMP) based. The term “ping” is used to indicate an echo request and an echo reply message.

Examples	> mping 172.12.35.31

Related Commands	eping config logging buffered debugging show logging debug mobility handoff enable