



Cisco Wireless LAN Controller Command Reference

Software Release 7.0.116.0
April 2011

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-19843-03

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

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

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

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

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

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

Copyright © 2011 Cisco Systems, Inc.
All rights reserved



CONTENTS

Preface 5

Audience 5

Purpose 5

Organization 6

Conventions 6

Related Documentation 7

Obtaining Documentation and Submitting a Service Request 7

7

CHAPTER 1

Using the Command-Line Interface 1-1

CLI Command Keyboard Shortcuts 1-2

Using the Interactive Help Feature 1-3

Using the Help Command 1-3

Using the ? command 1-4

Using the partial? command 1-4

Using the partial command<tab> 1-5

Using the command ? 1-5

command keyword ? 1-6

CHAPTER 2

CLI Commands 2-1

Show Commands for Viewing the Configuration 2-2

Show Advanced 802.11 Commands 2-18

Show Access Point Commands 2-41

Show Client Commands 2-90

Show Media-Stream Commands 2-186

Show Mesh Commands 2-190

Show Mobility Commands 2-210

Show RADIUS Commands 2-235

Show Radio Frequency ID Commands 2-240

Show Rogue Commands 2-246

Show TACACS Commands 2-279

Show WPS Commands 2-296

Configuring Controller Settings 2-308

Configure 802.11 Network Commands 2-308

Configure 802.11 Public Safety Commands	2-308
Configure 802.11b Commands	2-313
Configure 802.11h Commands	2-316
Configure 802.11 11n Support Commands	2-320
Configure 802.11 Antenna Commands	2-327
Configure 802.11 CleanAir Commands	2-335
Configure 802.11 CAC Commands	2-340
Configure Advanced 802.11 Commands	2-388
Configure Advanced 802.11 Channel Commands	2-390
Configure Advanced 802.11 Coverage Commands	2-403
Configure Advanced 802.11 Logging Commands	2-414
Configure Advanced 802.11 Monitor Commands	2-422
Configure Advanced 802.11 Profile Commands	2-430
Configure Advanced Timers Commands	2-451
Configure Access Point Commands	2-459
Configure Band-Select Commands	2-523
Configure Client Commands	2-535
Configure Interface Group Commands	2-576
Configure Guest-LAN Commands	2-578
Configure Macfilter Commands	2-634
Configure Memory Monitor Commands	2-660
Configure Mesh Commands	2-663
Configure Management-User Commands	2-688
Configure Mobility Commands	2-693
Configure Message Log Level Commands	2-705
Configure Media-Stream Commands	2-711
Configure Net User Commands	2-721
Configure Network Commands	2-736
Configure Port Commands	2-771
Configure RADIUS Account Commands	2-788
Configure RADIUS Authentication Server Commands	2-798
Configure Rogue Commands	2-818
Configure SNMP Commands	2-842
Configure Spanning Tree Protocol Commands	2-857
Configure TACACS Commands	2-873
Configure Trap Flag Commands	2-883
Configure Watchlist Commands	2-898
Configure Wireless LAN Commands	2-903
Configure Wireless LAN Security Commands	2-947
Configure WPS Commands	2-986

Capwap Access Point Commands	2-999
Saving Configurations	2-1011
Clearing Configurations, Logfiles, and Other Actions	2-1013
Resetting the System Reboot Time	2-1044
Uploading and Downloading Files and Configurations	2-1049
Installing and Modifying Licenses	2-1073
Troubleshooting Commands	2-1081



Preface

This preface describes the audience, organization, and conventions of the *Cisco Wireless LAN Command Reference Guide, Release 7.0.116.0*. It also provides information on how to obtain other documentation. This chapter includes the following sections:

- [Audience, page 5](#)
- [Organization, page 6](#)
- [Organization, page 6](#)
- [Conventions, page 6](#)
- [Related Documentation, page 7](#)
- [Obtaining Documentation and Submitting a Service Request, page 7](#)

Audience

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

Purpose

This guide describes the tasks and commands available to configure and maintain Cisco wireless LAN controllers.



Note

This version of the *Cisco Wireless LAN Controller Command Reference* pertains specifically to controller software release 7.0.116.0.

Organization

This guide is organized into these chapters:

Chapter Title	Description
Chapter 1, “Using the Command-Line Interface”	Describes how to use the command-line interface (CLI) on the controller.
Chapter 2, “CLI Commands”	Provides detailed information about the CLI commands for the controller 7.0.116.0 release.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{x y z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note

Means *reader take note*.



Tip

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



Caution

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

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Related Documentation

These documents provide complete information about the Cisco Unified Wireless Network solution:

- *Quick Start Guide: Cisco 2100 Series Wireless LAN Controllers*
- *Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers*
- *Cisco 5500 Series Wireless Controller Installation Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless Control System Configuration Guide*
- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points, Release 7.0.116.0*
- *Quick Start Guide: Cisco Wireless Control System*
- Quick start guide and hardware installation guide for your specific lightweight access point

Click this link to browse to user documentation for the Cisco Unified Wireless Network solution:

<http://www.cisco.com/cisco/web/psa/default.html?mode=prod>

Obtaining Documentation and Submitting a Service Request

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

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

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



CHAPTER 1

Using the Command-Line Interface

The command-line interface (CLI) is a line-oriented user interface that provides commands for configuring, managing, and monitoring the Cisco wireless LAN controller. This chapter contains the following topics:

- [CLI Command Keyboard Shortcuts, page 2](#)
- [Using the Interactive Help Feature, page 3](#)

CLI Command Keyboard Shortcuts

Table 1-1 lists CLI keyboard shortcuts to help you enter and edit command lines on the controller.

Table 1-1 CLI Command Keyboard Shortcuts

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

Using the Interactive Help Feature

The question mark (?) character allows you to get the following type of help about the command at the command line. Table 1-2 lists the interactive help feature list.

Table 1-2 Interactive Help Feature List

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

Using the Help Command

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

help

Usage Guidelines

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

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

Examples

```
> help
HELP:
Special keys:
  DEL, BS... delete previous character
  Ctrl-A .... go to beginning of line
  Ctrl-E .... go to end of line
  Ctrl-F .... go forward one character
  Ctrl-B .... go backward one character
  Ctrl-D .... delete current character
  Ctrl-U, X. delete to beginning of line
  Ctrl-K .... delete to end of line
  Ctrl-W .... delete previous word
  Ctrl-T .... transpose previous character
  Ctrl-P .... go to previous line in history buffer
  Ctrl-N .... go to next line in history buffer
  Ctrl-Z .... return to root command prompt
  Tab, <SPACE> command-line completion
```

```
Exit      .... go to next lower command prompt
?         .... list choices
```

Using the ? command

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 ?

Usage Guidelines

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

Examples

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

```
> ?

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

Using the partial? command

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

partial command?

Usage Guidelines

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

Examples

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

```
> controller> config>ad?
The command that matches with the string “ad” is as follows:
advanced
```

Using the partial command<tab>

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

partial command<tab>

Usage Guidelines

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

Examples

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

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

Using the command ?

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

command ?

Usage Guidelines

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

Examples

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

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

Information similar to the following appears:

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

command keyword ?

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

Usage Guidelines

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

Examples

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

```
> controller>config acl cpu ?
```

Information similar to the following appears:

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



CHAPTER 2

CLI Commands

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

This chapter contains the commands available in the Cisco CLI release 7.0.116.0. The controllers currently covered are as follows:

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

This chapter contains the following sections:

- [Show Commands for Viewing the Configuration, page 2-2](#)
- [Configuring Controller Settings, page 2-308](#)
- [Saving Configurations, page 2-1011](#)
- [Clearing Configurations, Logfiles, and Other Actions, page 2-1013](#)
- [Uploading and Downloading Files and Configurations, page 2-1049](#)
- [Installing and Modifying Licenses, page 2-1073](#)
- [Troubleshooting Commands, page 2-1081](#)

Show Commands for Viewing the Configuration

To display Cisco wireless LAN controller options and settings, use the **show** commands.

- [Show Advanced 802.11 Commands, page 2-18](#)
- [Show Access Point Commands, page 2-41](#)
- [Show Client Commands, page 2-90](#)
- [Show Media-Stream Commands, page 2-186](#)
- [Show Mesh Commands, page 2-190](#)
- [Show Mobility Commands, page 2-210](#)
- [Show RADIUS Commands, page 2-235](#)
- [Show Radio Frequency ID Commands, page 2-240](#)
- [Show Rogue Commands, page 2-246](#)
- [Show TACACS Commands, page 2-279](#)
- [Show WPS Commands, page 2-296](#)

Show 802.11 Commands

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

- `show 802.11{a | b | h}`
- `show 802.11{a | b | h} cleanair config`
- `show 802.11{a | b | h} cleanair air-quality summary`
- `show 802.11{a | b | h} cleanair air-quality worst`
- `show 802.11{a | b | h} cleanair device ap cisco_ap`
- `show 802.11{a | b | h} cleanair device type device_type`
- `show 802.11{a | b} cu-metrics cisco_ap`
- `show 802.11{a | b | h} cleanair config`

show 802.11

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

show 802.11{a | b | h}

Syntax Description

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

Defaults

None.

Examples

This example shows to display basic 802.11a network settings:

```
> show 802.11 a

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

--More-- or (q)uit
    MCS 6..... Supported
    MCS 7..... Supported
    MCS 8..... Supported
    MCS 9..... Supported
    MCS 10..... Supported
    MCS 11..... Supported
    MCS 12..... Supported
    MCS 13..... Supported
    MCS 14..... Supported
    MCS 15..... Supported
802.11n Status:
    A-MPDU Tx:
        Priority 0..... Enabled
        Priority 1..... Disabled
        Priority 2..... Disabled
        Priority 3..... Disabled
```

```

Priority 4..... Disabled
Priority 5..... Disabled
Priority 6..... Disabled
Priority 7..... Disabled
Beacon Interval..... 100
CF Pollable mandatory..... Disabled
CF Poll Request mandatory..... Disabled

--More-- or (q)uit
CFP Period..... 4
CFP Maximum Duration..... 60
Default Channel..... 36
Default Tx Power Level..... 0
DTPC Status..... Enabled
Fragmentation Threshold..... 2346
TI Threshold..... -50
Legacy Tx Beamforming setting..... Disabled
Traffic Stream Metrics Status..... Enabled
Expedited BW Request Status..... Disabled
World Mode..... Enabled
EDCA profile type..... default-wmm
Voice MAC optimization status..... Disabled
Call Admission Control (CAC) configuration
Voice AC:
  Voice AC - Admission control (ACM)..... Disabled
  Voice max RF bandwidth..... 75
  Voice reserved roaming bandwidth..... 6
  Voice load-based CAC mode..... Disabled
  Voice tspec inactivity timeout..... Disabled
  Voice Stream-Size..... 84000
  Voice Max-Streams..... 2
Video AC:

--More-- or (q)uit
  Video AC - Admission control (ACM)..... Disabled
  Video max RF bandwidth..... Infinite
  Video reserved roaming bandwidth..... 0

```

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

```

> show 802.11h

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

```

Related Commands

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

show 802.11 cleanair

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

show 802.11{a | b | h} cleanair config

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	h	Specifies the 802.11h network.
	config	Displays the network cleanair configuration.

Defaults None.

Examples This example shows how to display the 802.11a cleanair configuration:

```
> show 802.11a cleanair config
```

```
Clean Air Solution..... Enabled
Air Quality Settings:
  Air Quality Reporting..... Enabled
  Air Quality Reporting Period (min)..... 15
  Air Quality Alarms..... Enabled
  Air Quality Alarm Threshold..... 35
Interference Device Settings:
Interference Device Types:
  TDD Transmitter..... Disabled
  Jammer..... Disabled
  Continuous Transmitter..... Disabled
  DECT-like Phone..... Disabled
  Video Camera..... Disabled
  WiFi Inverted..... Disabled
  WiFi Invalid Channel..... Disabled
  SuperAG..... Disabled
  Radar..... Disabled
  Canopy..... Disabled
  WiMax Mobile..... Disabled
  WiMax Fixed..... Disabled

Interference Device Alarms..... Enabled
Interference Device Types Triggering Alarms:
  TDD Transmitter..... Disabled
  Jammer..... Disabled
  Continuous Transmitter..... Disabled
  DECT-like Phone..... Disabled
  Video Camera..... Disabled
  WiFi Inverted..... Disabled
  WiFi Invalid Channel..... Disabled
  SuperAG..... Disabled
  Radar..... Disabled
  Canopy..... Disabled
  WiMax Mobile..... Disabled
  WiMax Fixed..... Disabled
Additional Clean Air Settings:
CleanAir Event-driven RRM State..... Enabled
CleanAir Driven RRM Sensitivity..... Medium
```

```
CleanAir Persistent Devices state..... Disabled
```

Related Commands

[config 802.11 cleanair alarm](#)
[config 802.11 cleanair device](#)
[show 802.11 cleanair air-quality summary](#)
[show 802.11 cleanair device ap](#)
[show 802.11 cleanair device type](#)

show 802.11 cleanair air-quality summary

To display the air quality summary information for the 802.11 networks, use the **show 802.11 cleanair air-quality summary** command.

show 802.11{a | b | h} cleanair air-quality summary

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.
summary	Displays a summary of 802.11 radio band air quality information.

Defaults

None.

Examples

This example shows how to display a summary of the air quality information for the 802.11a network:

```
> show 802.11a cleanair air-quality summary
```

AQ = Air Quality

DFS = Dynamic Frequency Selection

AP Name	Channel	Avg AQ	Min AQ	Interferers	DFS
CISCO_AP3500	36	95	70	0	
CISCO_AP3500	40	93	75	0	

Related Commands

[config 802.11 cleanair alarm](#)
[config 802.11 cleanair device](#)
[show 802.11 cleanair](#)
[show 802.11 cleanair device ap](#)
[show 802.11 cleanair device type](#)

show 802.11 cleanair air-quality worst

To display the worst air quality information for the 802.11 networks, use the **show 802.11 cleanair air-quality worst** command.

show 802.11{a | b | h} cleanair air-quality worst

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.
worst	Displays the worst air quality information for 802.11 networks.

Defaults

None.

Examples

This example shows how to display worst air quality information for the 802.11a network:

```
> show 802.11a cleanair air-quality worst
```

AQ = Air Quality

DFS = Dynamic Frequency Selection

AP Name	Channel	Avg AQ	Min AQ	Interferers	DFS
CISCO_AP3500	1	83	57	3	5

Related Commands

[config 802.11 cleanair alarm](#)
[config 802.11 cleanair device](#)
[show 802.11 cleanair](#)
[show 802.11 cleanair device ap](#)
[show 802.11 cleanair device type](#)

show 802.11 cleanair device ap

To display the information of the device access point on the 802.11 radio band, use the **show 802.11 cleanair device ap** command.

show 802.11{a | b | h} cleanair device ap *cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.
<i>cisco_ap</i>	Specified access point name.

Defaults

None.

Examples

This example shows how to display the device access point for the 802.11a network:

```
> show 802.11a cleanair device ap AP_3500
```

DC = Duty Cycle (%)

ISI = Interference Severity Index (1-Low Interference, 100-High Interference)

RSSI = Received Signal Strength Index (dBm)

DevID = Device ID

No	ClusterID	DevID	Type	AP Name	ISI	RSSI	DC	Channel
1	c2:f7:40:00:00:03	0x8001	DECT phone	CISCO_AP3500	1	-43	3	149,153,157,161
2	c2:f7:40:00:00:51	0x8002	Radar	CISCO_AP3500	1	-81	2	153,157,161,165
3	c2:f7:40:00:00:03	0x8005	Canopy	CISCO_AP3500	2	-62	2	153,157,161,165

Related Commands

[config 802.11 cleanair alarm](#)
[config 802.11 cleanair device](#)
[show 802.11 cleanair](#)
[show 802.11 cleanair air-quality summary](#)
[show 802.11 cleanair device type](#)

show 802.11 cleanair device type

To display the information of all the interferers device type detected by a specific access point on the 802.11 radio band, use the **show 802.11 cleanair device type** command.

show 802.11{a | b | h} cleanair device type device_type

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.
<i>device_type</i>	Interferer device type for a specified radio band. The device type is one of the following: - tdd-tx—Tdd-transmitter device information. - jammer—Jammer device information. - cont-tx—Continuous-transmitter devices information. - dect-like—Dect-like phone devices information. - video—Video devices information. 802.11-inv—WiFi inverted devices information. 802.11-nonstd—Nonstandard WiFi devices information. - superag—Superag devices information. - canopy—Canopy devices information. - wimax-mobile—WiMax mobile devices information. - wimax-fixed—WiMax fixed devices information.

Defaults

None.

Examples

This example shows how to display the information of all the interferers detected by a specified access point for the 802.11a network:

```
> show 802.11a cleanair device type Canopy
```

DC = Duty Cycle (%)

ISI = Interference Severity Index (1-Low Interference, 100-High Interference)

RSSI = Received Signal Strength Index (dBm)

DevID = Device ID

No	ClusterID	DevID	Type	AP Name	ISI	RSSI	DC	Channel
1c2:f7:40:00:00:03	0x8005	Canopy	CISCO_AP3500	2	-62	2	153,157,161,165	

show 802.11 cu-metrics

To display access point channel utilization metrics, use the **show 802.11 cu-metrics** command.

show 802.11{a | b} cu-metrics *cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
<i>cisco_ap</i>	Access point name.

Defaults

None.

Examples

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

```
> show 802.11a cu-metrics myAP1

AP Interface Mac:          30:37:a6:c8:8a:50
Measurement Duration:      90sec

Timestamp                  Thu Jan 27 09:08:48 2011

Channel Utilization stats
=====
Picc (50th Percentile)..... 0
Pib (50th Percentile)..... 76
Picc (90th Percentile)..... 0
Pib (90th Percentile)..... 77

Timestamp                  Thu Jan 27 09:34:34 2011
```

show 802.11 media-stream

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

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

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	h	Specifies the 802.11h network.
	<i>media_stream_name</i>	Specified media stream name.

Defaults None.

Examples This example shows how to display the media-stream configuration:

```
> show 802.11a media-stream rrc
```

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

Related Commands [Show Mesh Commands](#)
[show media-stream group summary](#)

show aaa auth

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

show aaa auth

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display the configuration settings for the AAA authentication server database:

```
> 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

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

Defaults

None.

Examples

This example shows how to display a summary of the access control lists:

```
> show acl summary
```

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

This example shows how to display the detailed information of the access control lists:

```
> 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 cpu](#)
[config acl create](#)
[config acl delete](#)

```
config interface acl  
config acl rule  
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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the access control lists on the CPU:

```
> 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 cpu config acl create 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

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

Defaults

None.

Examples

This example shows how to display the automatic channel assignment configuration and statistics:

```
> show advanced 802.11a channel
```

Automatic Channel Assignment

```
Channel Assignment Mode..... AUTO
Channel Update Interval..... 600 seconds [startup]
Anchor time (Hour of the day)..... 0
Channel Update Contribution..... SNI.
Channel Assignment Leader..... 00:1a:6d:dd:1e:40
Last Run..... 129 seconds ago
```

```
DCA Sensitivity Level: ..... STARTUP (5 dB)
```

Channel Energy Levels

```
Minimum..... unknown
Average..... unknown
Maximum..... unknown
```

Channel Dwell Times

```
Minimum..... unknown
Average..... unknown
Maximum..... unknown
```

```
Auto-RF Allowed Channel List..... 36,40,44,48,52,56,60,64,149,
..... 153,157,161
```

```
Auto-RF Unused Channel List..... 100,104,108,112,116,132,136,
..... 140,165,190,196
```

```
DCA Outdoor AP option..... Enabled
```

Related Commands

[config advanced 802.11 channel add](#)
[config advanced 802.11 channel cleanair-event](#)
[config advanced 802.11 channel dca anchor-time](#)
[config advanced 802.11 channel dca chan-width-11n](#)
[config advanced 802.11 channel dca interval](#)
[config advanced 802.11 channel dca sensitivity](#)
[config advanced 802.11 channel foreign](#)
[config advanced 802.11 channel load](#)
[config advanced 802.11 channel noise](#)

■ show advanced 802.11 channel

config advanced 802.11 channel update
show advanced 802.11 channel

show advanced 802.11 coverage

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

show advanced 802.11{a | b} coverage

Syntax Description

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

Defaults

None.

Examples

This example shows how to display the statistics for coverage hole detection:

```
> 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

[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](#)
[config advanced 802.11 coverage rssi-threshold](#)
[show advanced 802.11 coverage](#)

show advanced 802.11 group

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

show advanced 802.11{a | b} group

Syntax Description

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

Defaults

None.

Examples

This example shows how to display Cisco radio RF group settings:

```
> 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

[config advanced 802.11 group-mode](#)

show advanced 802.11 l2roam

To display 802.11a or 802.11b/g Layer 2 client roaming information, use the **show advanced 802.11 l2roam** command.

show advanced 802.11{a | b} l2roam {rf-param | statistics mac_address}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
rf-param	Specifies the Layer 2 frequency parameters.
statistics	Specifies the Layer 2 client roaming statistics.
<i>mac_address</i>	MAC address of the client.

Defaults

None.

Examples

This example shows how 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

[config 802.11 l2roam rf-params](#)

show advanced 802.11 logging

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

show advanced 802.11{a | b} logging

Syntax Description

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

Defaults

None.

Examples

This example shows how to display 802.11b RF event and performance logging:

```
> 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

[config advanced 802.11 logging channel](#)
[config advanced 802.11 logging coverage](#)
[config advanced 802.11 logging foreign](#)
[config advanced 802.11 logging load](#)
[config advanced 802.11 logging noise](#)
[config advanced 802.11 logging performance](#)
[config advanced 802.11 logging txpower](#)
[show advanced 802.11 channel](#)

show advanced 802.11 monitor

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

show advanced 802.11{a | b} monitor

Syntax Description

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

Defaults

None.

Examples

This example shows how to display the radio monitoring for the 802.11b network:

```
> show advanced 802.11b monitor
```

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

Related Commands

[config advanced 802.11 monitor load](#)
[config advanced 802.11 monitor mode](#)
[config advanced 802.11 monitor noise](#)
[config advanced 802.11 monitor signal](#)

show advanced 802.11 profile

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

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Specifies all Cisco lightweight access points.
<i>cisco_ap</i>	Name of a specific Cisco lightweight access point.

Defaults

None.

Examples

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
> 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
```

This example shows how to display the configuration and statistics of a specific access point profile:

```
> 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

[config advanced 802.11 profile clients](#)
[config advanced 802.11 profile customize](#)
[config advanced 802.11 profile foreign](#)
[config advanced 802.11 profile noise](#)

show advanced 802.11 receiver

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

show advanced 802.11{a | b} receiver

Syntax Description

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

Defaults

None.

Examples

This example shows how to display the configuration and statistics of the 802.11a network settings:

```
> 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

[config advanced 802.11 profile clients](#)

show advanced 802.11 summary

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

show advanced 802.11{a | b} summary

Syntax Description

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

Defaults

None.

Examples

This example shows how to display a summary of the 802.11b access point settings:

```
> 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

[config advanced 802.11 7920VSIEConfig](#)
[config advanced 802.11 channel add](#)
[show advanced 802.11 channel](#)

show advanced 802.11 txpower

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

show advanced 802.11{a | b} txpower

Syntax Description

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

Defaults

None.

Examples

This example shows how to display the configuration and statistics of the 802.11b transmit power cost:

```
> 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

[config advanced 802.11 txpower-update](#)

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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display the backup controller information:

> **show advanced backup-controller**

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

Related Commands [config advanced backup-controller primary](#)
[config advanced backup-controller secondary](#)

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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the client auto handoff mode after excessive retries:

```
> show advanced client-handoff
```

```
Client auto handoff after retries..... 130
```

Related Commands	config advanced client-handoff show advanced 802.11 summary

show advanced dot11-padding

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

show advanced dot11-padding

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to view the state of over-the-air frame padding:

```
> 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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the EAP settings:

```
> show advanced eap
```

```
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries..... 20
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 1
EAP-Request Max Retries..... 20
EAPOL-Key Timeout (milliseconds)..... 1000
EAPOL-Key Max Retries..... 2
```

Related Commands	config advanced eap config advanced timers eap-identity-request-delay config advanced timers eap-timeout

show advanced max-1x-sessions

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

show advanced max-1x-sessions

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the maximum 802.1X sessions per access point:

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

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

Related Commands	show advanced statistics

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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the probe settings for the WLAN controller:

```
> 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	config advanced probe filter config advanced probe limit

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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the switch control path rate limiting mode:

> **show advanced rate**

Control Path Rate Limiting..... Disabled

Related Commands	config advanced rate config advanced eap

show advanced send-disassoc-on-handoff

To display whether the WLAN controller disassociates clients after a handoff, use the **show advanced send-disassoc-on-handoff** command.

show advanced send-disassoc-on-handoff

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

```
> show advanced send-disassoc-on-handoff
```

```
Send Disassociate on Handoff..... Disabled
```

show advanced sip-preferred-call-no

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

show advanced sip-preferred-call-no

Syntax Description This command has no arguments or keywords.

Defaults None.

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

```
> show advanced sip-preferred-call-no
```

```
Preferred Call Numbers List
```

Call Index	Preferred Call No
-----	-----
1	911
2	100
3	101
4	102
5	103
6	104

show advanced 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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display switch port statistics mode: <pre>> show advanced statistics</pre> Switch port statistics..... Enabled

Related Commands	config advanced statistics

show advanced timers

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

show advanced timers

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are shown in the “Examples” section.

Examples

This example shows how to display the system timers setting:

```
> 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

[config advanced timers ap-discovery-timeout](#)
[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 eap-identity-request-delay](#)
[config advanced timers eap-timeout](#)

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	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults None.

Examples This example shows how to display auto-RF information for an access point:

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

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

```

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

```

show ap ccx rm

To display an access point's Cisco Client eXtensions (CCX) radio management status information, use the **show ap ccx rm** command.

show ap ccx rm *ap_name* status

Syntax Description

<i>ap_name</i>	Specified access point name.
<i>status</i>	Displays the CCX radio management status information for an access point.

Defaults

None.

Examples

This example shows how to display the status of the CCX radio management:

```
> 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

[config ap](#)
[show ap ccx rm](#)

show ap cdp

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

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

Syntax Description

all	Displays the CDP status on all access points.
ap-name	Displays the CDP status for a specified access point.
neighbors	Displays neighbors using CDP.
detail	Displays details about a specific access point neighbor using CDP.
<i>cisco_ap</i>	Specified access point name.

Defaults

None.

Examples

This example shows how to display the CDP status of all access points:

```
> show ap cdp all
```

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

This example shows how to display the CDP status of a specified access point:

```
> show ap cdp ap-name SB_RAP1
```

```
AP CDP State
AP Name          AP CDP State
-----
AP CDP State.....Enabled
AP Interface-Based CDP state
  Ethernet 0.....Enabled
  Slot 0.....Enabled
  Slot 1.....Enabled
```

This example shows how to display details about all neighbors using CDP:

```
> 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

This example shows how to display details about a specific neighbor with a specified access point using CDP:

```
> 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

This example shows how to display details about neighbors using CDP:

```
> 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	<i>ap_name</i>	Name of the mesh access point.

Defaults	None.

Examples This example shows how to display the available channels for a particular access point:

```
> 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	802.11a	Specifies the 802.11a or 802.11b/g network.
	802.11b	Specifies the 802.11b/g network.
	general	Displays general access point settings.
	<i>cisco_ap</i>	Lightweight access point name.

Defaults None.

Examples This example shows how to display the detailed configuration for an access point:

> **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%

```

■ show ap config

```

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

```

This example shows how to display the detailed configuration for another access point:

> **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

```

This example shows how to display the general configuration of a Cisco access point:

```
> show ap config general cisco-ap
```

```

Cisco AP Identifier..... 9
Cisco AP Name..... cisco-ap

```

■ show ap config

```

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

Ethernet Port Duplex..... Auto
Ethernet Port Speed..... Auto
AP Link Latency..... Enabled
  Current Delay..... 0 ms
  Maximum Delay..... 240 ms
  Minimum Delay..... 0 ms
  Last updated (based on AP Up Time)..... 4 days, 06 h 17 m 20 s
Rogue Detection..... Enabled
AP TCP MSS Adjust..... Disabled
Mesh preferred parent..... 00:24:13:0f:92:00

```

Related Commands

[config ap](#)
[show ap config global](#)

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	The command has no arguments and keywords.

Defaults	None.

Examples	This example shows how to display global syslog server settings: <pre>> show ap config global</pre> AP global system logging host..... 255.255.255.255

Related Commands	config ap show ap config

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

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

Defaults

None.

Examples

This example shows how to display memory core dump information:

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

```
Memory core dump is disabled.
```

Related Commands

[config ap core-dump](#)
[show ap crash-file](#)

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 This example shows how to display the crash file generated by the access point:

```
> show ap crash-file
```

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](#)

show ap data-plane

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

show ap data-plane {all | cisco_ap}

Syntax Description

all	Specifies all Cisco lightweight access points.
<i>cisco_ap</i>	Name of a Cisco lightweight access point.

Defaults

None.

Examples

This example shows how to display the data plane status of all access points:

> **show ap data-plane all**

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

show ap eventlog

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

show ap eventlog *ap_name*

Syntax Description

<i>ap_name</i>	Event log for the specified access point.

Defaults

None.

Examples

This example shows how to display the event log of an access point:

```
> show ap eventlog CiscoAP
AP event log download has been initiated
Waiting for download to complete

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

show ap image

To display the detailed information about the predownloaded image for specified access points, use the **show ap image** command.

show ap image {*cisco_ap* | **all**}

Syntax Description

<i>cisco_ap</i>	Name of the lightweight access point.
all	Specifies all access points.



Note

If you have an AP that has the name *all*, it conflicts with the keyword **all** that specifies all access points. In this scenario, the keyword **all** takes precedence over the AP that is named *all*.

Defaults

None.

Examples

This example shows how to display images present on all access points:

```
> show ap image all
```

```
Total number of APs..... 7
Number of APs
Initiated..... 4
Predownloading..... 0
Completed predownloading..... 3
Not Supported..... 0
Failed to Predownload..... 0
```

AP Name	Primary Image	Backup Image	Status	Version	Next Retry Time	Retry Count
AP1140-1	7.0.56.0	6.0.183.38	Complete	6.0.183.38	NA	NA
AP1140-2	7.0.56.0	6.0.183.58	Initiated	6.0.183.38	23:46:43	1
AP1130-2	7.0.56.0	6.0.183.38	Complete	6.0.183.38	NA	NA
AP1130-3	7.0.56.0	6.0.183.58	Initiated	6.0.183.38	23:43:25	1
AP1130-4	7.0.56.0	6.0.183.38	Complete	6.0.183.38	NA	NA
AP1130-5	7.0.56.0	6.0.183.58	Initiated	6.0.183.38	23:43:00	1
AP1130-6	7.0.56.0	6.0.183.58	Initiated	6.0.183.38	23:41:33	

Related Commands

[config ap image predownload](#)
[config ap image swap](#)

show ap inventory

To display inventory information for an access point, use the **show ap inventory** command.

show ap inventory *ap_name*

Syntax Description

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

Defaults

None.

Examples

This example shows how to display the inventory of an access point:

```
> show ap inventory test101
```

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

show ap join stats detailed

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

show ap join stats detailed *ap_mac*

Syntax Description	<i>ap_mac</i>	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.

Defaults	None.

Examples	This example shows how to display join information for a specific access point trying to join the controller:

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

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

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

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

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

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

■ show ap join stats detailed**Related Commands**

[show ap join stats detailed](#)
[show ap join stats summary](#)
[show ap join stats summary all](#)

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	<i>ap_mac</i>	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.

Defaults	None.

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

Examples	This example shows how to display specific join information for an access point: <pre>> show ap join stats summary 00:0b:85:02:0d:20</pre> 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	show ap join stats detailed show ap join stats summary all

show ap join stats summary all

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

show ap join stats summary all

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display a summary of join information for all access points:

```
> 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 [show ap join stats detailed](#)
[show ap join stats summary](#)

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 link-encryption** command.

show ap link-encryption {all | cisco_ap}

Syntax Description

all	Specifies all access points.
cisco_ap	Name of the lightweight access point.

Defaults

None.

Examples

This example shows how to display the link encryption status of all access points:

```
> 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

[config ap link-encryption](#)
[config ap link-latency](#)

show ap monitor-mode summary

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

show ap monitor-mode summary

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display current channel-optimized monitor mode settings:

```
> 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 [config ap mode](#)
[config ap monitor-mode](#)

show ap retransmit

To display access point control packet retransmission parameters, use the **show ap retransmit** command.

show ap retransmit {**all** | *cisco_ap*}

Syntax Description

all	Specifies all access points.
<i>cisco_ap</i>	Specifies the name of the access point.

Defaults

None.

Examples

This example shows how to display the control packet retransmission parameters of all access points on a network:

```
> show ap retransmit all
```

Global control packet retransmit interval: 3 (default)

Global control packet retransmit count: 5 (default)

AP Name	Retransmit Interval	Retransmit count
AP_004	3 (default)	5 (WLC default),5 (AP default)

Related Commands

[config ap retransmit interval](#)

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 [tsm {client_mac | all}]

Syntax Description	802.11a	Specifies the 802.11a network
	802.11b	Specifies the 802.11b/g network.
	wlan	Specifies WLAN statistics.
	<i>cisco_ap</i>	Specifies the name of the lightweight access point.
	tsm	Specifies the traffic stream metrics.
	<i>client_mac</i>	MAC address of the client.
	all	Specifies all access points.

Defaults None.

Examples This example shows how to display statistics of an access point for the 802.11b network:

```
> show ap stats 802.11b AP02
```

```

Number Of Slots..... 2
AP Name..... 1140_LAP_1
MAC Address..... c4:7d:4f:3a:35:53
Radio Type..... RADIO_TYPE_80211b/g
Stats Information
  Number of Users..... 3
  TxFragmentCount..... 232095
  MulticastTxFrameCnt..... 3834
  FailedCount..... 347196
  RetryCount..... 683429
  MultipleRetryCount..... 21416
  FrameDuplicateCount..... 0
  RtsSuccessCount..... 20
  RtsFailureCount..... 0
  AckFailureCount..... 439834
  RxIncompleteFragment..... 0
  MulticastRxFrameCnt..... 0
  FcsErrorCount..... 5845734
  TxFrameCount..... 232095
  WepUndecryptableCount..... 0
  TxFramesDropped..... 22
Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw)..... 50
  Total channel MT free..... 0
  Total voice MT free..... 0
  Na Direct..... 0
  Na Roam..... 0
  Video Bandwidth in use(% of config bw)..... 0
WMM TSPEC CAC Call Stats
  Total num of voice calls in progress..... 1
  Num of roaming voice calls in progress..... 1
  Total Num of voice calls since AP joined..... 13
  Total Num of roaming calls since AP joined..... 13

```

```

Total Num of exp bw requests received..... 0
Total Num of exp bw requests admitted..... 0
Num of voice calls rejected since AP joined.... 0
Num of roam calls rejected since AP joined..... 1
Num of calls rejected due to insufficient bw.... 0
Num of calls rejected due to invalid params.... 0
Num of calls rejected due to PHY rate..... 0
Num of calls rejected due to QoS policy..... 0
SIP CAC Call Stats
  Total Num of calls in progress..... 1
  Num of roaming calls in progress..... 0
Total Num of calls since AP joined..... 29
  Total Num of roaming calls since AP joined..... 2
Total Num of Preferred calls received..... 0
  Total Num of Preferred calls accepted..... 0
  Total Num of ongoing Preferred calls..... 0
  Total Num of calls rejected(Insuff BW)..... 0
  Total Num of roam calls rejected(Insuff BW).... 0
Band Select Stats
  Num of dual band client ..... 0
  Num of dual band client added..... 0
  Num of dual band client expired ..... 0
  Num of dual band client replaced..... 0
  Num of dual band client detected ..... 0
  Num of suppressed client ..... 0
  Num of suppressed client expired..... 0
  Num of suppressed client replaced..... 0

```

Related Commands

[config ap static-ip](#)
[config ap stats-timer](#)

show ap summary

To display a summary of all lightweight access points attached to the controller, use the **show ap summary** command.

show ap summary [*cisco_ap*]

Syntax Description

cisco_ap

(Optional) Type sequence of characters that make up the name of a specific AP or a group of APs, or enter a wild character search pattern.

Defaults

None.

Usage Guidelines

A list that contains each lightweight access point name, number of slots, manufacturer, MAC address, location, and the controller port number appears. When you specify

Examples

This example shows how to display a summary of all connected access points:

> show ap summary

Number of APs..... 2

Global AP username..... user

Global AP Dot1x username..... Not Configured

Number of APs..... 2

Global AP username..... user

Global AP Dot1x username..... Not Configured

AP Name	Slots	AP Model	Ethernet MAC	Location	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

config ap

show ap tcp-mss-adjust

To display the Transmission Control Protocol (TCP) maximum segment size (MSS) information of access points, use the **show ap tcp-mss-adjust** command.

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

Syntax Description

<i>cisco_ap</i>	Specified lightweight access point name.
all	Specifies all access points.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

None.

Examples

This example shows how to display Transmission Control Protocol (TCP) maximum segment size (MSS) information of all access points:

```
> 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 Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point, use the **show ap wlan** command.

show ap wlan 802.11{a | b} cisco_ap

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
<i>ap_name</i>	Lightweight access point name.

Defaults

None.

Examples

This example shows how to display BSSIDs of an access point for the 802.11b network:

```
> 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

[config ap wlan](#)

show arp kernel

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

show arp kernel

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

> **show arp kernel**

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

Related Commands	clear arp debug arp show route kernel

show arp switch

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

show arp switch

Syntax Description This command has no arguments or keywords.

Defaults None.

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

> **show arp switch**

MAC Address	IP Address	Port	VLAN	Type
xx:xx:xx:xx:xx:xx	xxx.xxx.xxx.xxx	service port	1	
xx:xx:xx:xx:xx:xx	xxx.xxx.xxx.xxx	service port		
xx:xx:xx:xx:xx:xx	xxx.xxx.xxx.xxx	service port		

Related Commands

- [clear arp](#)
- [debug arp](#)
- [show arp kernel](#)

show auth-list

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

show auth-list

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the access point authorization list:

> **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	

Related Commands	clear tacacs 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 This command has no arguments or keywords.

Defaults None.

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

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

> **show boot**

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

Related Commands [config boot](#)

show cac voice summary

To view the list of all AP's along with brief Voice statistics. It includes Bandwidth used, Max bandwidth available and number of calls information, use the **show cac voice summary** command.

show cac voice summary

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the list of all AP's along with brief Voice statistics:

> **show cac voice summary**

AP Name	Slot#	Radio	BW Used/Max	Calls
APc47d.4f3a.3547	0	11b/g	0/23437	0
	1	11a	1072/23437	1

Related Commands	show mesh cac

show call-control ap



Note

The **show call-control ap** command is applicable only for SIP based calls.

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

802.11a	Specifies the 802.11a network
802.11b	Specifies the 802.11b/g network.
<i>cisco_ap</i>	Cisco access point name.
metrics	Specifies the call metrics information.
traps	Specifies the trap information for call control.

Defaults

None.

Examples

This example shows how to display the metrics for successful calls generated for an access point:

```
> 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
```

This example shows how to display the metrics for the traps generated for an access point:

```
> 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
```

Usage Guidelines

To aid in troubleshooting, the output of this command shows an error code for any failed calls. [Table 2-1](#) explains the possible error codes for failed calls.

Table 2-1 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.

Table 2-1 Error Codes for Failed VoIP Calls (continued)

Error Code	Integer	Description
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.
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.
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.

Table 2-1 **Error Codes for Failed VoIP Calls (continued)**

Error Code	Integer	Description
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.
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.

show call-control client

To see call information for a call-aware client when Voice-over-IP (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

callInfo	Specifies the call-control information.
<i>client_MAC_address</i>	Client MAC address.

Defaults

None.

Examples

This example shows how to display the call information such as the IP port for calls related to the client:

```
> show call-control client callInfo 10.10.10.10.10.10
```

```
Uplink IP/port..... 0.0.0.0 / 0
Downlink IP/port..... 9.47.96.107 / 5006
UP..... 6
Calling Party..... sip:1021
Called Party..... sip:1000
Call ID..... 38423970c3fca477
Call on hold: ..... FALSE
Number of calls for given client is..... 1
```

Related Commands

[show call-control ap](#)

show capwap client config

To display the list of clients associated with the CAPWAP access point, use the **show capwap client** command.

show capwap client config

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display clients associated with CAPWAP access point:

```
> show capwap client config

configMagicMark      0xF1E2D3C4
chkSumV2             23845
chkSumV1             43434
swVer                4.2.37.156
adminState           ADMIN_ENABLED(1)
name                 AP001b.0cfc.3f80
location             default location
group name
mwarName             WLC1
mwarIPAddress        9.41.80.67
mwarName
mwarIPAddress        0.0.0.0
mwarName
mwarIPAddress        0.0.0.0
ssh status           Disabled
Telnet status        Disabled
numOfSlots           2
spamRebootOnAssert   1
spamStatTimer        180
randSeed             0x0
transport             SPAM_TRANSPORT_L3(2)
transportCfg         SPAM_TRANSPORT_DEFAULT(0)
initialisation       SPAM_PRODUCTION_DISCOVERY(1)
```

Related Commands

- [capwap ap ip address](#)
- [capwap ap ip default-gateway](#)
- [show capwap client ip config](#)

show capwap client ip config

To display the CAPWAP static IP configuration, use the **show capwap client ip config** command.

show capwap client ip config

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the CAPWAP static IP information:

```
> show capwap client config
```

```
LWAPP Static IP Configuration  
Primary Controller 9.41.80.88
```

Related Commands	capwap ap controller ip address capwap ap ip address show capwap client config

show capwap reap association

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

show capwap reap association

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display clients associated to an access point and their SSIDs:

```
> show capwap 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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the status of the hybrid-REAP access point: <pre>> show capwap reap status</pre>

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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display the status of the compatibility mode:

```
> 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 a Locally Significant Certificate (LSC), use the **show certificate lsc summary** command.

show certificate lsc {summary | ap-provision}

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

Defaults None.

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

```
> show certificate lsc summary
```

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

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

```
> show certificate lsc ap-provision
```

```
LSC AP-Provisioning..... Yes
Provision-List..... Present

Idx Mac Address
---
1 00:18:74:c7:c0:90
```

Related Commands

- [config certificate](#)
- [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	This command has no arguments or keywords.

Defaults	None.

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

```
> show certificate summary
```

```
Web Administration Certificate..... Locally Generated
Web Authentication Certificate..... Locally Generated
Certificate compatibility mode:..... off
```

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

show route kernel

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

show route kernel

Syntax Description This command has no arguments or keywords.

Defaults None.

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

```
> show route kernel
```

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

Related Commands

- [clear arp](#)
- [debug arp](#)
- [show arp kernel](#)
- [config route add](#)
- [config route delete](#)

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	802.11a	Specifies the 802.11a network.
	802.11b	Specifies the 802.11b/g network.
	<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults None.

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

Examples This example shows how to display client information on an access point:

```
> 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 country](#)
- [show exclusionlist](#)

show client calls

To display the total number of active or rejected calls on the controller, use the **show client calls** command.

show client calls {active | rejected} {802.11a | 802.11b/g | all}

Syntax Description	active	Displays active calls.
	rejected	Displays rejected calls.
	802.11a	Specifies the 802.11a network.
	802.11b/g	Specifies the 802.11b/g network.
	all	Specifies both the 802.11a and 802.11b/g network.

Defaults None.

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

```
> show client calls active 802.11a
```

Client MAC	Username	Total Call Duration (sec)	AP Name	Radio Type
00:09: ef: 02:65:70	abc	45	VJ-1240C-ed45cc	802.11a
00:13: ce: cc: 51:39	xyz	45	AP1130-a416	802.11a
00:40:96: af: 15:15	def	45	AP1130-a416	802.11a
00:40:96:b2:69: df	def	45	AP1130-a416	802.11a

Number of Active Calls ----- 4

Related Commands [debug voice-diag](#)

show client ccx client-capability

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

show client ccx client-capability *client_mac_address*

Syntax Description	<i>client_mac_address</i> MAC address of the client.

Defaults	None.

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

Examples	This example shows how to display the client's capability: <pre>> show client ccx client-capability 00:40:96:a8:f7:98</pre> <pre>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)</pre>

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 display 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	
	<i>client_mac_address</i> MAC address of the client.

Defaults	
	None.

Examples	
	This example shows how to display the data frame sent from the client for the last test: > show client ccx frame-data xx:xx:xx:xx:xx:xx

show client ccx last-response-status

To display 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

client_mac_address MAC address of the client.

Defaults

None.

Examples

This example shows how to display the status of the last test response:

```
> 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 clear-reports](#)
[config client ccx clear-results](#)
[config client ccx default-gw-ping](#)
[config client ccx dhcp-test](#)
[config client ccx log-request](#)
[show client ccx last-response-status](#)
[show client ccx last-test-status](#)

show client ccx last-test-status

To display 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	<i>client_mac_address</i> MAC address of the client.

Defaults	None.

Examples	This example shows how to display the status of the last test of the client:

```
> 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 clear-reports config client ccx clear-results config client ccx default-gw-ping config client ccx dhcp-test config client ccx log-request show client ccx last-response-status

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	roam	(Optional) Displays the CCX client roaming log response.
	rsna	(Optional) Displays the CCX client RSNA log response.
	syslog	(Optional) Displays the CCX client system log response.
	<i>client_mac_address</i>	Inventory for the specified access point.

Defaults None.

Examples This example shows how to display the system log response:

```
> 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'
```

This example shows how to display the client roaming log response:

```
> 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
```

■ show client ccx log-response

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

show client ccx manufacturer-info

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

show client ccx manufacturer-info *client_mac_address*

Syntax Description	<i>client_mac_address</i> MAC address of the client.

Defaults	None.

Examples This example shows how to display the client manufacturing information:

```
> 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, MaxRss1:-30
Rx Sensitivity ..... Rate:2.0 Mbps, MinRssi:-95, MaxRss1:-30
Radio Type ..... HRDSSS(802.11b)
Rx Sensitivity ..... Rate:5.5 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ..... Rate:11.0 Mbps, MinRssi:-95, MaxRss1:-30
Radio Type ..... ERP(802.11g)
Rx Sensitivity ..... Rate:6.0 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ..... Rate:9.0 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ..... Rate:12.0 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ..... Rate:18.0 Mbps, MinRss1:-95, MaxRss1:-30

```

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 operating-parameters

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

show client ccx operating-parameters *client_mac_address*

Syntax Description

<i>client_mac_address</i>	MAC address of the client.

Defaults

None.

Examples

This example shows how to display the client operating parameters:

```
> 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 display the client profiles, use the **show client ccx profiles** command.

show client ccx profiles *client_mac_address*

Syntax Description	<i>client_mac_address</i> MAC address of the client.

Defaults	None.

Examples	This example shows how to display the client profiles: <pre>> show client ccx profiles 00:40:96:a8:f7:98</pre> <pre> 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 </pre>

■ show client ccx profiles

```

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

show client ccx results *client_mac_address*

Syntax Description	<i>client_mac_address</i> MAC address of the client.

Defaults	None.

Examples	This example shows how to display the results from last successful diagnostic test:

```
> show client ccs results xx.xx.xx.xx
```

```
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 Cisco Client eXtension (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 | beacon | pathloss}}
```

Syntax Description

<i>client_MAC</i>	Client MAC address.
status	Displays the client CCX radio management status information.
report	Displays the 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.
pathloss	Displays radio management path loss reports.

Defaults

None.

Examples

This example shows how to display the client radio management status information:

```
> 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
```

This example shows how to display the client radio management load reports:

```
> 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
```


This example shows how to display the client radio management noise histogram reports:

```
> 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
```

Related Commands

[config client ccx default-gw-ping](#)
[config client ccx dhcp-test](#)

show client ccx stats-report

To display the Cisco Client eXtensions (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

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

Defaults

None.

Examples

This example shows how to displays the statistics report:

```
> 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-test](#)
[config client ccx dns-ping](#)

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

Defaults	None.

Usage Guidelines	The show client ap command may list the status of automatically disabled clients. Use the show exclusionlist command to display clients on the exclusion list (blacklisted).

Examples	This example shows how to display the client detailed information:

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

Policy Manager State.....POSTURE_REQD
Policy Manager Rule Created.....Yes
Client MAC Address..... 00:16:36:40:ac:58
Client Username..... N/A
Client State..... Associated
Client NAC OOB State..... QUARANTINE
Guest LAN Id..... 1
IP Address..... Unknown
Session Timeout..... 0
QoS Level..... Gold
Diff Serv Code Point (DSPC)..... disabled
Mobility State..... Local
Internal Mobility State..... apfMsMmInitial
Security Policy Completed..... No
Policy Manager State..... WEBAUTH_REQD
Policy Manager Rule Created..... Yes
NPU Fast Fast Notified..... Yes
Last Policy Manager State..... WEBAUTH_REQD
Client Entry Create Time..... 460 seconds
Interface..... wired-guest
H-REAP Authentication..... Local
H-REAP Data Switching..... Local
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
```

show client detail

```
Number of Policy Errors..... 0
Radio Signal Strength Indicator..... Unavailable
Signal to Noise Ratio..... Unavailable
...
```

Related Commands [show client summary](#)

show client location-calibration summary

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

show client location-calibration summary

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the location calibration summary information:

```
> 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 summary show client summary guest-lan

show client probing

To display the number of probing clients, use the **show client probing** command.

show client probing

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the number of probing clients:

```
> show client probing
```

```
Number of Probing Clients..... 0
```

Related Commands	show client summary show client summary guest-lan

show client roam-history

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

show client roam-history *mac_address*

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

Defaults	None.

Examples	This example shows how to display the roaming history of a specified client: > show client roam-history 00:14:6c:0a:57:77

show client summary

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

show client summary

Syntax Description This command has no arguments or keywords.

Defaults None.

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

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

```
> show client summary
```

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

MAC Address	AP Name	Status	WLAN/GLAN/RLAN	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 summary guest-lan](#)

show client summary guest-lan

To display the active wired guest LAN clients, use the **show client summary guest-lan** command.

show client summary guest-lan

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

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

```
Number of Clients..... 1
MAC Address      AP Name      Status      WLAN  Auth  Protocol  Port Wired
-----
00:16:36:40:ac:58  N/A        Associated    1     No    802.3     1     Yes
```

Related Commands	show client summary

show client tsm

To display the client traffic stream metrics (TSM) statistics, use the **show client tsm** command.

show client tsm 802.11 {a | b} client_mac {ap_mac | all}

Syntax Description	802.11a	Specifies the 802.11a network.
	802.11b	Specifies the 802.11 b/g network.
	<i>client_mac</i>	MAC address of the client.
	<i>ap_mac</i>	MAC address of the tsm access point.
	all	Specifies the list of all access points to which the client has associations.

Defaults None.

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

```
> show client tsm 802.11a xx:xx:xx:xx:xx:xx all

AP Interface MAC: 00:0b:85:01:02:03
Client Interface Mac:          00:01:02:03:04:05
Measurement Duration:          90 seconds

Timestamp                      1st Jan 2006, 06:35:80
UpLink Stats
=====
Average Delay (5sec intervals).....35
Delay less than 10 ms.....20
Delay bet 10 - 20 ms.....20
Delay bet 20 - 40 ms.....20
Delay greater than 40 ms.....20
Total packet Count.....80
Total packet lost count (5sec).....10
Maximum Lost Packet count(5sec).....5
Average Lost Packet count(5secs).....2
DownLink Stats
=====
Average Delay (5sec intervals).....35
Delay less than 10 ms.....20
Delay bet 10 - 20 ms.....20
Delay bet 20 - 40 ms.....20
Delay greater than 40 ms.....20
Total packet Count.....80
Total packet lost count (5sec).....10
Maximum Lost Packet count(5sec).....5
Average Lost Packet count(5secs).....2
```

Related Commands

- [show client ap](#)
- [show client detail](#)
- [show client summary](#)

show client username

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

show client username *username*

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

Defaults	None.

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

```
> show client username IT_007
```

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

Related Commands	show client ap show client detail show client summary

show client voice-diag

To display voice diagnostics statistics, use the **show client voice-diag** command.

show client voice-diag {quos-map | roam-history | rssi | status | tspec}

Syntax Description		
quos-map		Displays information about the QoS/DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.
roam-history		Displays information about the last 3 roaming history. The output contains the Timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, reason for roaming-failure.
rssi		Display the client's RSSI values in the last 5 seconds when voice diagnostics is enabled.
status		Displays status of voice diagnostics for clients.
tspec		Displays TSPEC for voice diagnostic clients.

Defaults None.

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

```
> show client voice-diag status
```

```
Voice Diagnostics Status: FALSE
```

Related Commands

- [show client ap](#)
- [show client detail](#)
- [show client summary](#)
- [debug voice-diag](#)

show country

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

show country

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the configured countries and supported radio types:

> **show country**

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

Related Commands	config country show country channels show country supported

show country channels

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

show country channels

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display the auto-RF channels for the configured countries:

> **show country channels**

```
Configured Country..... United States
KEY: * = Channel is legal in this country and may be configured manually.
     A = Channel is the Auto-RF default in this country.
     . = Channel is not legal in this country.
     C = Channel has been configured for use by Auto-RF.
     x = Channel is available to be configured for use by Auto-RF.
-----:+++++
802.11BG :
Channels :          1 1 1 1 1
          : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----:+++++
      US : A * * * * A * * * * A . . .
-----:+++++
802.11A :  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels : 3 3 3 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
          : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----:+++++
      US : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
-----:+++++
```

Related Commands

- [config country](#)
- [show country](#)
- [show country supported](#)

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.

Defaults None.

Examples This example shows how to display a list of all the supported countries:

```
> show country supported
```

```
Configured Country..... United States
Supported Country Codes
AR - Argentina..... 802.11a / 802.11b / 802.11g
AT - Austria..... 802.11a / 802.11b / 802.11g
AU - Australia..... 802.11a / 802.11b / 802.11g
BR - Brazil..... 802.11a / 802.11b / 802.11g
BE - Belgium..... 802.11a / 802.11b / 802.11g
BG - Bulgaria..... 802.11a / 802.11b / 802.11g
CA - Canada..... 802.11a / 802.11b / 802.11g
CH - Switzerland..... 802.11a / 802.11b / 802.11g
CL - Chile..... 802.11b / 802.11g
CN - China..... 802.11a / 802.11b / 802.11g
CO - Colombia..... 802.11b / 802.11g
CY - Cyprus..... 802.11a / 802.11b / 802.11g
CZ - Czech Republic..... 802.11a / 802.11b
DE - Germany..... 802.11a / 802.11b / 802.11g
DK - Denmark..... 802.11a / 802.11b / 802.11g
EE - Estonia..... 802.11a / 802.11b / 802.11g
ES - Spain..... 802.11a / 802.11b / 802.11g
FI - Finland..... 802.11a / 802.11b / 802.11g
FR - France..... 802.11a / 802.11b / 802.11g
GB - United Kingdom..... 802.11a / 802.11b / 802.11g
GI - Gibraltar..... 802.11a / 802.11b / 802.11g
GR - Greece..... 802.11a / 802.11b / 802.11g
HK - Hong Kong..... 802.11a / 802.11b / 802.11g
HU - Hungary..... 802.11a / 802.11b / 802.11g
ID - Indonesia..... 802.11b / 802.11g
IE - Ireland..... 802.11a / 802.11b / 802.11g
IN - India..... 802.11a / 802.11b / 802.11g
IL - Israel..... 802.11a / 802.11b / 802.11g
ILO - Israel (outdoor)..... 802.11b / 802.11g
IS - Iceland..... 802.11a / 802.11b / 802.11g
IT - Italy..... 802.11a / 802.11b / 802.11g
JP - Japan (J)..... 802.11a / 802.11b / 802.11g
J2 - Japan 2(P)..... 802.11a / 802.11b / 802.11g
J3 - Japan 3(U)..... 802.11a / 802.11b / 802.11g
KR - Korea Republic (C)..... 802.11a / 802.11b / 802.11g
KE - Korea Extended (K)..... 802.11a / 802.11b / 802.11g
LI - Liechtenstein..... 802.11a / 802.11b / 802.11g
LT - Lithuania..... 802.11a / 802.11b / 802.11g
LU - Luxembourg..... 802.11a / 802.11b / 802.11g
LV - Latvia..... 802.11a / 802.11b / 802.11g
```

show country supported

```

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](#)
[show country](#)
[show country channels](#)

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.

Defaults	None.

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

```
> show coredump summary
```

```
Core Dump is enabled
FTP Server IP..... 10.10.10.17
FTP Filename..... file1
FTP Username..... ftpuser
FTP Password..... *****
```

Related Commands	config coredump config coredump ftp config coredump username

show cpu

To display current WLAN controller CPU usage information, use the **show cpu** command.

show cpu

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

> **show cpu**

Current CPU load: 2.50%

show custom-web

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

show custom-web

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

```
> show custom-web
```

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

Related Commands	config custom-web ext-webauth-mode config custom-web ext-webauth-url config custom-web ext-webserver config custom-web redirectUrl config custom-web webauth-type config custom-web weblogo config custom-web webmessage config custom-web webtitle

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.

Defaults	None.

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

```
> show database summary
```

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

Related Commands	config database size

show debug

To determine if the MAC address and other flag debugging is enabled or disabled, sse the **show debug** command.

show debug

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display if debugging is enabled:

```
> show debug

MAC debugging..... disabled

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

Related Commands	debug mac

show dhcp

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

show dhcp {**detailed** | **leases** | **opt-82** | **proxy** | **stats** | **summary** | **timeout** | *scope*}

Syntax Description

show	Display settings.
dhcp	Dynamic Host Configuration Protocol settings.
detailed	Enter detailed to display DHCP information for a particular scope. DHCP scope name allows space by using double quote like "scope 003".
leases	Enter leases to display allocated DHCP leases.
proxy	Enter proxy to display the status if DHCP proxy.
stats	Enter stats to display the DHCP proxy statistics.
summary	Enter summary to display DHCP summary information.
timeout	Enter timeout to display the DHCP timeout information.
<i>scope</i>	Enter the name of a scope to display the DHCP information for that scope.

Defaults

None.

Examples

This example shows how to display the allocated DHCP leases:

```
> show dhcp leases
```

No leases allocated.

This example shows how to display the DHCP summary information:

```
> show dhcp summary
```

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

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

```
> show dhcp 003
```

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

Related Commands

[config dhcp](#)
[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

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

show dtls connections

Syntax Description This command has no arguments or keywords.

Defaults None.

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

> **show dtls connections**

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

show dhcp proxy

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

show dhcp proxy

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

```
> show dhcp proxy
```

```
DHCP Proxy Behavior: enabled
```

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

show dhcp timeout

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

show dhcp timeout

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

```
> show dhcp timeout
```

```
DHCP Timeout (seconds)..... 10
```

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

show eventlog

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

show eventlog

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display the event log entries:

```
> show eventlog
```

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

show 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 This command has no arguments or keywords.

Defaults None.

Usage Guidelines This command displays all manually excluded MAC addresses.

Examples This example shows how to display the exclusion list:

```
> show exclusionlist
```

```
No manually disabled clients.
```

```
Dynamically Disabled Clients
```

```
-----
MAC Address           Exclusion Reason           Time Remaining (in secs)
-----
00:40:96:b4:82:55     802.1X Failure            51
```

Related Commands [config exclusionlist](#)

show guest-lan

To display the configuration of a specific wired guest LAN, use the **show guest-lan** command.

show guest-lan *guest_lan_id*

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

Defaults	None.

Usage Guidelines	To display <i>all</i> wired guest LANs configured on the controller, use the show guest-lan summary command.

Examples	This example shows how to display the guest LAN configuration:

```
> show guest-lan 2

Guest LAN Identifier..... 1
Profile Name..... guestlan
Network Name (SSID)..... guestlan
Status..... Enabled
AAA Policy Override..... Disabled
Number of Active Clients..... 1
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... wired
Ingress Interface..... wired-guest
WLAN ACL..... unconfigured
DHCP Server..... 10.20.236.90
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
Security
  Web Based Authentication..... Enabled
  ACL..... Unconfigured
  Web-Passthrough..... Disabled
  Conditional Web Redirect..... Disabled
  Auto Anchor..... Disabled
Mobility Anchor List
GLAN ID IP Address Status
```

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

show 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

<i>group_name</i>	IP address of hybrid-REAP group.

Defaults

None.

Examples

This example shows how to display the detailed information for a specific hybrid-REAP group:

```
> 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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the current list of hybrid-REAP groups:

```
> 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

summary	Displays a list of all OfficeExtend access points.
latency	Displays the link delay for OfficeExtend access points.

Defaults

None.

Examples

This example shows how to display information about the list of hybrid-REAP officeExtend access points:

```
> 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
```

This example shows how to display the hybrid-REAP officeExtend access point's link delay:

```
> 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	brief	Displays a brief summary of all active IKE SAs.
	detailed	Displays a detailed summary of all active IKE SAs.
	<i>IP_or_MAC_address</i>	IP or MAC address of active IKE SA.

Defaults None.

Examples This example shows how to display the active Internet Key Exchange security associations:

```
> show ike brief 10.10.10.10
```

show interface

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

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

Syntax Description

summary	Displays a summary of the local interfaces.
detailed	Displays detailed interface information.
<i>interface_name</i>	Interface name for detailed display.

Defaults

None.

Examples

This example shows how to display a summary of the local interfaces:

```
> 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	

This example shows how to display the detailed interface information:

```
> 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

[show interface group](#)

show interface group

To display details of system interface groups, use the **show interface group** command:

show interface group {**summary** | **detailed** *interface_group_name*}

Syntax Description	summary	Displays a summary of the local interface groups.
	detailed	Displays detailed interface group information.
	<i>interface_group_name</i>	Interface group name for a detailed display.

Defaults None.

Examples This example shows how to display a summary of local interface groups:

```
> show interface group summary
```

Interface Group Name	Total Interfaces	Total WLANs	Total AP Groups	Quarantine
mygroup1	1	0	0	No
mygroup2	1	0	0	No
mygroup3	5	1	0	No

This example shows how to display the detailed interface group information:

```
> show interface group detailed mygroup1
```

```
Interface Group Name..... mygroup1
Quarantine ..... No
Number of Wlans using the Interface Group..... 0
Number of AP Groups using the Interface Group.... 0
Number of Interfaces Contained..... 1
Interface Group Description..... My Interface Group
Next interface for allocation to client..... testabc
Interfaces Contained in this group ..... testabc
```

Interface marked with * indicates DHCP dirty interface

Related Commands [show interface](#)
[config interface group](#)

show invalid-config

To see any ignored commands or invalid configuration values in an edited configuration file, use the **show invalid-config** command.

show invalid-config

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Usage Guidelines

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

Examples

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

```
> show invalid-config
```

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

show inventory

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

show inventory

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

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

```
> show inventory

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

Related Commands	show ap inventory

show 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	brief	Displays a brief summary of active IPsec SAs.
	detailed	Displays a detailed summary of active IPsec SAs.
	<i>IP_or_MAC_address</i>	IP address or MAC address of a device.

Defaults None.

Examples This example shows how to display brief information about the active Internet Protocol Security (IPsec) security associations (SAs):

```
> 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	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.

Defaults None.

Examples This example shows how to display a summary of all known access points:

```
> 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

summary	Displays all L2TP sessions.
<i>ip_address</i>	IP address.

Defaults

None.

Examples

This example shows how to display a summary of all L2TP sessions:

```
> show l2tp summary
```

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

```


show lag eth-port-hash

To display the physical port used for specific MAC addresses, use the **show lag eth-port-hash** command.

show lag eth-port-hash *dest_MAC* [*source_MAC*]

Syntax Description

<i>dest_MAC</i>	MAC address to determine output port for non-IP packets.
<i>source_MAC</i>	(Optional) MAC address to determine output port for non-IP packets.

Defaults

None.

Examples

This example shows how to display the physical port used for a specific MAC address:

```
> show lag eth-port-hash 11:11:11:11:11:11
```

Destination MAC 11:11:11:11:11:11 currently maps to port 1

Related Commands

[config lag](#)

show lag ip-port-hash

To display the physical port used for specific IP addresses, use the **show lag ip-port-hash** command.

show lag ip-port-hash *dest_IP* [*source_IP*]

Syntax Description

<i>dest_IP</i>	IP address to determine output port for IP packets.
<i>source_IP</i>	(Optional) IP address to determine output port for IP packets.

Defaults

None.

Usage Guidelines

For CAPWAP packets, enter the AP's IP address. For EOIP packets, enter the WLC's IP address. For WIRED_GUEST packets, enter its IP address. For nontunnelled IP packets from WLC, enter the destination IP address. For other nontunnelled IP packets, enter both destination and source IP addresses.

Examples

This example shows how to display the physical port used for a specific IP address:

```
> show lag ip-port-hash 192.168.102.138
```

```
Destination IP 192.168.102.138 currently maps to port 1
```

Related Commands

[config lag](#)

show lag summary

To display the current link aggregation (LAG) status, use the **show lag summary** command.

show lag summary

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the current status of the LAG configuration: <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

index LDAP server index. Valid values are from 1 to 17.

Defaults

None.

Examples

This example shows how to display the detailed LDAP server information:

```
> 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

This command has no arguments or keywords:

Examples

This example shows how to display the LDAP server statistics:

```
> 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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display a summary of configured LDAP servers:

> **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	counters	Displays license agent counter information.
	sessions	Display session information.

Defaults	None.

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

```
> show license agent counters
```

```
License Agent Counters
Request Messages Received:0: Messages with Errors:0
Request Operations Received:0: Operations with Errors:0
Notification Messages Sent:0: Transmission Errors:0: Soap Errors:0
```

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

```
> show license agent sessions
```

```
License Agent Sessions: 0 open, maximum is 9
```

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

show license all

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

show license all

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Examples

This example shows how to display all the licenses:

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



```
StoreIndex: 3 Feature: base-ap-count Version: 1.0
License Type: Evaluation
License State: Active, Not in Use, EULA accepted
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 3 days
License Count: 250/0/0
License Priority: Low
```

Related Commands

- [license install](#)
- [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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display the license capacity:

> **show license capacity**

Licensed Feature	Max Count	Current Count	Remaining Count

AP Count	250	47	203

Related Commands

- [license install](#)
- [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	<i>license-name</i>	Name of a specific license.

Defaults	None.

Examples	This example shows how to display the license details:

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

Related Commands	license install 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

This command has no arguments or keywords.

Defaults

None.

Examples

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

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

Related Commands

[license install](#)
[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	This command has no arguments or keywords.

Defaults	None.

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

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

Related Commands	license install 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 This command has no arguments or keywords.

Defaults None.

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

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

Related Commands

- [license install](#)
- [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 file** command.

show license file

Syntax Description

This command has no arguments or keywords.

Examples

This example shows how to display the license files:

```
> show license file
License Store: Primary License Storage
Store Index: 0
License: 11 wplus-ap-count 1.0 LONG NORMAL STANDALONE EXCL 12_KEYS INFINIT
E_KEYS NEVER NEVER NiL SLM_CODE CL_ND_LCK NiL *1AR5NS7M5AD8PPU400
NiL NiL NiL 5_MINS <UDI><PID>AIR-CT5508-K9</PID><SN>RFD000P2D27<
/SN></UDI> Pe0L7tv8KDUqo:z1Pe423S5wasgM8G,tTs0i,7zLyA3VfxhnIe5aJa
m63lR5l8JM3DPkr4O2DI43iLlKn7jomo3RF1lLjMRqLkKHiLJ2tOyuftQSQ2bCAO6
nR3wIb38xKi3t$<WLC>AQEBIQAB//++mCzRUbOhw28vz0czAY0iAm7ocDLUMb9ER0
+BD3w2PhNEYwsBN/T3xXBqJqfC+oKRqWInXo3s+nsLU7rOtdOxoIxYZAo3LYmUJ+M
Fzsq1hKoJVlPyEvQ8H21MNUjVbhoN0gyIWsyiJaM8AQIkVBQFzhr10GYolVzdzfJf
EPQIx6tZ++/Vtc/q3SF/5Ko8XCy=</WLC>

Comment:
Hash: iOGjuLlXgLhcTB113ohIzxVioHA=

. . .
```

Related Commands

[license install](#)
[show license all](#)
[show license detail](#)
[show license expiring](#)
[show license feature](#)
[show license image-level](#)
[show license in-use](#)
[show license summary](#)

show license handle

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

show license handle

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Examples

This example shows how to display the license handles:

```
> show license handle
```

```
Feature: wplus                               , Handle Count: 1
      Units: 01( 0), ID: 0x5e000001, NotifyPC: 0x1001e8f4 LS-Handle (0x00000001),
Units: ( 1)

      Registered clients: 1
      Context 0x1051b610, epID 0x10029378
Feature: base                               , Handle Count: 0
      Registered clients: 1
      Context 0x1053ace0, epID 0x10029378
Feature: wplus-ap-count                     , Handle Count: 1
      Units: 250( 0), ID: 0xd4000002, NotifyPC: 0x1001e8f4      LS-Handle (0x000
00002), Units: (250)

      Registered clients: None
Feature: base-ap-count                       , Handle Count: 0
      Registered clients: None
Global Registered clients: 2
      Context 0x10546270, epID 0x100294cc
      Context 0x1053bae8, epID 0x100294cc
```

Related Commands

[license install](#)
[show license all](#)
[show license detail](#)
[show license expiring](#)
[show license feature](#)
[show license image-level](#)
[show license in-use](#)
[show license summary](#)

show license image-level

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

show license image-level

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

```
> show license image-level
Module name  Image level  Priority  Configured  Valid license
wnbu         wplus       1        YES        wplus
             base        2        NO
```

NOTE: wplus includes two additional features: Office Extend AP, Mesh AP.

Related Commands	license install 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 This command has no arguments or keywords.

Defaults None.

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

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

Related Commands

- [license install](#)
- [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	This command has no arguments or keywords.

Defaults	None.

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

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

Related Commands	license install 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 the license status on the Cisco 5500 Series Controller, use the **show license status** command.

show license status

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display the license status:

```
> show license status
      License Type Supported
permanent  Non-expiring node locked license
extension  Expiring node locked license
evaluation  Expiring non node locked license

      License Operation Supported
install    Install license
clear      Clear license
annotate   Comment license
save       Save license
revoke     Revoke license

      Device status
Device Credential type: DEVICE
Device Credential Verification: PASS
Rehost Type: DC_OR_IC
```

Related Commands

- [license install](#)
- [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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the license statistics:

```
> show license statistics
      Administrative statistics
      Install success count:      0
      Install failure count:     0
      Install duplicate count:   0
      Comment add count:         0
      Comment delete count:      0
      Clear count:               0
      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 This command has no arguments or keywords.

Defaults None.

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

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

Related Commands

- [license install](#)
- [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	This command has no arguments or keywords.

Defaults	None.

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

```
> show license udi
```

Device#	PID	SN	UDI

*0	AIR-CT5508-K9	RFD000P2D27	AIR-CT5508-K9:RFD000P2D27

Related Commands	license install 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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the load-balancing status:

```
> show load-balancing
```

```
Aggressive Load Balancing..... Enabled
Aggressive Load Balancing Window..... 0 clients
Aggressive Load Balancing Denial Count..... 3
Statistics
Total Denied Count..... 10 clients
Total Denial Sent..... 20 messages
Exceeded Denial Max Limit Count..... 0 times
None 5G Candidate Count..... 0 times
None 2.4G Candidate Count..... 0 times
```

Related Commands	config load-balancing

show local-auth certificates

To display local authentication certificate information, use the **show local-auth certificates** command:

show local-auth certificates

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the authentication certificate information stored locally:

```
> 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-ac-s-a.cisco.com
Issuer: C=AU, ST=NSW, L=Sydney, O=Cisco Systems
OU=WNBU Sydney, CN=wnbu-syd-ac-s-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-ac-s-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
```

show local-auth certificates

```
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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the local authentication configuration information:

```
> 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 ..... 7b7fffffff000000000000000000000000
    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

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

show local-auth statistics

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display the local authentication certificate statistics:

```
> 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](#)

■ show local-auth statistics

```
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	detail	(Optional) Displays detailed location information.
	<i>mac_address</i>	MAC address of a client.
	summary	(Optional) Displays summary location information.

Defaults None.

Examples This example shows how to display the location summary information:

```
> 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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display the detailed location RFID statistics:

> **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 This command has no arguments or keywords.

Defaults None.

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

> **show logging**

```
Logging to buffer :
- Logging of system messages to buffer :
  - Logging filter level..... errors
  - Number of system messages logged..... 67227
  - Number of system messages dropped..... 21136
- Logging of debug messages to buffer ..... Disabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
Logging to console :
- Logging of system messages to console :
  - Logging filter level..... errors
  - Number of system messages logged..... 0
  - Number of system messages dropped..... 88363
- Logging of debug messages to console ..... Enabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
Logging to syslog :
- Syslog facility..... local0
- Logging of system messages to syslog :
  - Logging filter level..... errors
  - Number of system messages logged..... 67227
--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
```

show logging

```
packet from 1.100.163.51. Source member:0.0.0.0. source member unknown.  
*Apr 03 09:47:34.194: %LWAPP-3-DECODE_ERR: spam_lrad.c:1271 Error decoding discovery  
request from AP 00:13:5f:0e:d4:20  
*Apr 03 09:47:34.194: %LWAPP-3-DISC_OTAP_ERR: spam_lrad.c:5554 Ignoring OTAP discovery  
request from AP 00:13:5f:0e:d4:20, OTAP is disabled  
Previous message occurred 2 times.
```

Related Commands

[config logging syslog host](#)
[config logging syslog facility](#)
[config logging syslog level](#)

show login session

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

show login session

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

> **show login session**

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

Related Commands	config login session close

show macfilter

To display the MAC filter parameters, use the **show macfilter** command.

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

Syntax Description

summary	Displays a summary of all MAC filter entries.
detail <i>MAC</i>	Detailed display of a MAC filter entry.

Defaults

None.

Usage Guidelines

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.

Examples

This example shows how to display the detailed display of a MAC filter entry:

```
> 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
```

This example shows how to display a summary of the MAC filter parameters:

```
> 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 interfac](#)
[config macfilter ip-address](#)
[config macfilter mac-delimiter](#)
[config macfilter radius-compatible](#)
[config macfilter wlan-id](#)

show memory monitor

To display a summary of memory analysis settings and any discovered memory issues, use the **show memory monitor** command.

show memory monitor [detail]

Syntax Description	detail (Optional) Displays details of any memory leaks or corruption.
Defaults	None.
Usage Guidelines	Be careful when changing the defaults for the config memory monitor command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

Examples

This example shows how to display a summary of memory monitoring settings and a summary of test results:

```
> show memory monitor

Memory Leak Monitor Status:
low_threshold(10000), high_threshold(30000), current status(disabled)
-----
Memory Error Monitor Status:
Crash-on-error flag currently set to (disabled)
No memory error detected.
```

This example shows how to display the monitor test results:

```
> show memory monitor detail

Memory error detected. Details:
-----
- Corruption detected at pmalloc entry address:          (0x179a7ec0)
- Corrupt entry:headerMagic(0xdeadf00d),trailer(0xabcd),poison(0xreadceef),
entrysize(128),bytes(100),thread(Unknown task name,task id = (332096592)),
file(pmalloc.c),line(1736),time(1027)

Previous 1K memory dump from error location.
-----
(179a7ac0): 00000000 00000000 00000000 ceeff00d readf00d 00000080 00000000 00000000
(179a7ae0): 17958b20 00000000 1175608c 00000078 00000000 readceef 179a7afc 00000001
(179a7b00): 00000003 00000006 00000001 00000004 00000001 00000009 00000009 0000020d
(179a7b20): 00000001 00000002 00000002 00000001 00000004 00000000 00000000 5d7b9aba
(179a7b40): cbddf004 192f465e 7791acc8 e5032242 5365788c a1b7cee6 00000000 00000000
(179a7b60): 00000000 00000000 00000000 00000000 00000000 ceeff00d readf00d 00000080
(179a7b80): 00000000 00000000 17958dc0 00000000 1175608c 00000078 00000000 readceef
(179a7ba0): 179a7ba4 00000001 00000003 00000006 00000001 00000004 00000001 00003763
(179a7c00): 1722246c 1722246c 00000000 00000000 00000000 00000000 00000000 ceeff00d
(179a7c20): readf00d 00000080 00000000 00000000 179a7b78 00000000 1175608c 00000078
...
```

■ show memory monitor**Related Commands**

[config memory monitor errors](#)
[config memory monitor leaks](#)
[debug memory](#)

show reset

To display the scheduled system reset parameters, use the **show reset** command.

show reset

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

```
> show reset
```

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

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

show remote-lan

To display information about remote LAN configuration, use the **show remote-lan** command.

show remote-lan { **summary** | *remote-lan-id* }

Syntax Description

summary	Displays a summary of all remote LANs.
<i>remote-lan-id</i>	Remote LAN identifier.

Defaults

None.

Examples

This example shows how to display a summary of all remote LANs:

```
> show remote-lan summary
```

```
Number of Remote LANS..... 2
```

RLAN ID	RLAN Profile Name	Status	Interface Name
2	remote	Disabled	management
8	test	Disabled	management

This example shows configuration information about the remote LAN with the *remote-lan-id* 2:

```
> show remote-lan 2
```

```
Remote LAN Identifier..... 2
Profile Name..... remote
Status..... Disabled
MAC Filtering..... Disabled
AAA Policy Override..... Disabled
Network Admission Control

    Radius-NAC State..... Disabled
    SNMP-NAC State..... Disabled
    Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Number of Active Clients..... 0
Exclusionlist..... Disabled
Session Timeout..... Infinity
CHD per Remote LAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... management
Remote LAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Static IP client tunneling..... Disabled
Radius Servers
    Authentication..... Global Servers
    Accounting..... Global Servers
    Dynamic Interface..... Disabled
Security

    Web Based Authentication..... Enabled
    ACL..... Unconfigured
    Web Authentication server precedence:
```



```
1..... local
2..... radius
3..... ldap
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Disabled
```

Related Commands

[config memory monitor errors](#)
[config memory monitor leaks](#)
[debug memory](#)

Show Media-Stream Commands

Use the **show media-stream** commands to display the multicast-direct configuration state.

show media-stream client

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

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

Syntax Description	<i>media-stream_name</i>	Name of the media-stream client of which the details is to be displayed.
	summary	Displays the details for a set of media-stream clients.

Defaults None.

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

```
> show media-stream client summary
```

```
Number of Clients..... 1
```

Client Mac	Stream Name	Stream Type	Radio	WLAN	QoS	Status
00:1a:73:dd:b1:12	mountainview	MC-direct	2.4	2	Video	Admitted

Related Commands [show media-stream group summary](#)

show media-stream group detail

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

show media-stream group detail *media-stream_name*

Syntax Description	<i>media-stream_name</i>	Name of the media-stream group.

Defaults	None.

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

```
> show media-stream group detail abc
```

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

Related Commands	show media-stream group summary

show media-stream group summary

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

show media-stream group summary

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

```
> show media-stream group summary
```

Stream Name	Start IP	End IP	Operation Status
-----	-----	-----	-----
abc	227.8.8.8	227.9.9.9	Multicast-direct

Related Commands	Show Mesh Commands

Show Mesh Commands

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

show mesh ap

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

show mesh ap {summary | tree}

Syntax Description	summary	Displays a summary of mesh access point information including the 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 the name, hop counter, link signal-to-noise ratio (SNR), and bridge group name.

Defaults None.

Examples This example shows how to display a summary format:

```
> 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       sbbox
SB_MAP1  AIR-LAP1522AG-A-K9      00:1d:71:0e:85:00 00:1d:71:0e:85:00 1       sbbox
SB_MAP2  AIR-LAP1522AG-A-K9      00:1b:d4:a7:8b:00 00:1b:d4:a7:8b:00 2       sbbox
SB_MAP3  AIR-LAP1522AG-A-K9      00:1d:71:0d:ee:00 00:1d:71:0d:ee:00 3       sbbox

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

```

This example shows how to display settings in a hierarchical (tree) format:

```
> 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
-----

```

■ show mesh ap

Related Commands

[config mesh alarm](#)
[config mesh astools](#)
[config mesh battery-state](#)

show mesh astools stats

To display antistranding statistics for outdoor mesh access points, use the **show mesh astools stats** command.

show mesh astools stats [*cisco_ap*]

Syntax Description	<i>cisco_ap</i> (Optional) Antistranding feature statistics for a designated mesh access point.

Defaults	None.

Examples This example shows how to display anti-stranding statistics on all outdoor mesh access points:

```
> show mesh astools stats
```

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

This example shows how to display anti-stranding statistics for access point *sb_map1*:

```
> 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 backhaul

To check the current backhaul, use the **show mesh backhaul** command.

show mesh backhaul *cisco_ap*

Syntax Description

<i>cisco_ap</i>	Name of the access point.

Defaults

None.

Examples

This example shows how to display the current backhaul:

```
> show mesh backhaul ap_abc
```

If the current backhaul is 5 GHz, the output is as follows:

```
Basic Basic Attributes for Slot 0
  Radio Type..... RADIO_TYPE_80211g
  Radio Role..... DOWNLINK_ACCESS
  Administrative State ..... ADMIN_ENABLED
  Operation State ..... UP
  Current Tx Power Level ..... 1
```

If the current backhaul is 2.4 GHz, the output is as follows:

```
Basic Attributes for Slot 1
  Radio Type..... RADIO_TYPE_80211a
  Radio Subband..... RADIO_SUBBAND_ALL
  Radio Role..... DOWNLINK_ACCESS
  Administrative State ..... ADMIN_ENABLED
  Operation State ..... UP
  Current Tx Power Level ..... 1
  Current Channel ..... 165
  Antenna Type..... EXTERNAL_ANTENNA
  External Antenna Gain (in .5 dBm units).... 0
Current Channel.....6
Antenna Type.....Externa_ANTENNA
External Antenna Gain (in .5 dBm units).....0
```

Related Commands

[config mesh battery-state](#)
[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** command.

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

Syntax Description

summary	Displays the total number of voice calls and voice bandwidth used for each mesh access point.
bwused	Displays the bandwidth for a selected access point in a tree topology.
voice	Displays the mesh topology and the voice bandwidth used or available.
video	Displays the mesh topology and the video bandwidth used or available.
access	Displays access voice calls in progress in a tree topology.
callpath	Displays the call bandwidth distributed across the mesh tree.
rejected	Displays voice calls rejected for insufficient bandwidth in a tree topology.
<i>cisco_ap</i>	Mesh access point name.

Defaults

None.

Examples

This example shows how to display a summary of the call admission control settings:

```
> 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

This example shows how to display the mesh topology and the voice bandwidth used or available:

```
> 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

This example shows how to display the access voice calls in progress in a tree topology:

```
> 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
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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display backhaul client access configuration settings for a mesh access point:

```
> show mesh client-access
```

```
Backhaul with client access status: enabled
```

```
Backhaul with client access extended status(3 radio AP): disabled
```

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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display global mesh configuration settings:

> **show mesh config**

```
Mesh Range..... 12000
Mesh Statistics update period..... 3 minutes
Backhaul with client access status..... disabled
Backhaul with extended client access status..... disabled
Background Scanning State..... enabled
Backhaul Amsdu State..... disabled

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..... disabled

Mesh DCA channels for serial backhaul APs..... enabled
Mesh Slot Bias..... enabled
```

Related Commands

- [show mesh stats](#)
- [show mgmtuser](#)
- [config mesh alarm](#)

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		
summary		Displays global environment summary information.
<i>cisco_ap</i>		Name of access point for which environment summary information is requested.

Defaults None.

Examples This example shows how to display global environment summary information:

> **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

This example shows how to display an environment summary for an access point:

> **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 [show mesh stats](#)

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

detail	Displays the channel and signal-to-noise ratio (SNR) details between the designated mesh access point and its neighbor.
summary	Displays the mesh neighbors for a designated mesh access point.
<i>cisco_ap</i>	Cisco lightweight access point name.
all	Displays all access points.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Examples

This example shows how to display a neighbor summary of an access point:

```
> show mesh neigh summary RAP1
```

AP Name/Radio	Mac	Channel	Rate	Link-Snr	Flags	State
00:1D:71:0F:CA:00	157	54	6	0x0	BEACON	
00:1E:14:48:25:00	157	24	1	0x0	BEACON	
MAP1-BB00	157	54	41	0x11	CHILD BEACON	

This example shows how to display the detailed neighbor statistics of an access point:

```
> show mesh neigh detail RAP1
```

```
AP MAC : 00:1E:BD:1A:1A:00 AP Name: HOR1522_MINE06_MAP_S_Dyke
backhaul rate 54
FLAGS : 860 BEACON
worstDv 255, Ant 0, channel 153, biters 0, ppiters 0
Numroutes 0, snr 0, snrUp 8, snrDown 8, linkSnr 8
adjustedEase 0, unadjustedEase 0
txParent 0, rxParent 0
poorSnr 0
lastUpdate 2483353214 (Sun Aug 4 23:51:58 1912)
parentChange 0
Per antenna smoothed snr values: 0 0 0 0
Vector through 00:1E:BD:1A:1A:00
```

Table 2-2 lists the output flags displayed for the **config mesh linktest** command.

Table 2-2 Output Flags for the Config Mesh Linktest Command

Output Flag	Description
AP MAC	MAC address of a mesh neighbor for a designated mesh access point.
AP Name	Name of the mesh access point.

Table 2-2 **Output Flags for the Config Mesh Linktest Command (continued)**

Output Flag	Description
FLAGS	Describes adjacency. The possible values are as follows: • UPDATED—Recently updated neighbor. • NEIGH—One of the top neighbors. • EXCLUDED—Neighbor is currently excluded. • WASEXCLUDED—Neighbor was recently removed from the exclusion list. • PERMSNR—Permanent SNR neighbor. • CHILD—A child neighbor. • PARENT—A parent neighbor. • NEEDUPDATE—Not a current neighbor and needs an update. • BEACON—Heard a beacon from this neighbor. • ETHER—Ethernet neighbor.
worstDv	Worst distance vector through the neighbor.
Ant	Antenna on which the route was received.
channel	Channel of the neighbor.
biters	Number of black list timeouts left.
ppiters	Number of potential parent timeouts left.
Numroutes	Number of distance routes.
snr	Signal to Noise Ratio.
snrUp	SNR of the link to the AP.
snrDown	SNR of the link from the AP.
linkSnr	Calculated SNR of the link.
adjustedEase	Ease to the root AP through this AP. It is based on the current SNR and threshold SNR values.
unadjustedEase	Ease to the root AP through this AP after applying correct for number of hops.
txParent	Packets sent to this node while it was a parent.
rxparent	Packets received from this node while it was a parent.
poorSnr	Packets with poor SNR received from a node.
lastUpdate	Timestamp of the last received message for this neighbor
parentChange	When this node last became parent.
per antenna smoother SNR values	SNR value is populated only for antenna 0.

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

<i>cisco_ap</i>	Mesh access point name.

Defaults

None.

Examples

This example shows how to display channel and SNR details for a designated link path:

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

AP Name/Radio Mac	Channel	Rate	Link-Snr	Flags	State
MAP1-BB00	157	54	32	0x0	UPDATED NEIGH PARENT BEACON
RAP1	157	54	37	0x0	BEACON

Related Commands

[config mesh battery-state](#)
[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

<i>summary</i>	Displays the packet error rate stats summary.
<i>cisco_ap</i>	Name of mesh access point.
all	Displays all mesh access points.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

None.

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

This example shows how to display the percentage of packet errors for packets transmitted by the neighbors to a mesh access point:

```
> 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
RTS Attempts: 0
RTS Success: 0
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
RTS Attempts: 0
RTS Success: 0
```

Related Commands

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

show mesh queue-stats

To display 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

<i>cisco_ap</i>	Name of access point for which you want packet queue statistics.
all	Displays all access points.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

None.

Examples

This example shows how to display packet queue statistics for access point ap417:

```
> 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](#)
[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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to view 4.8-GHz public safety settings:

```
> 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 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

<i>cisco_ap</i>	Name of access point for which you want packet error statistics.
all	Displays all access points.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

None.

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

This example shows how to display packet error statistics for access point ap417:

```
> 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
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

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

Defaults

None.

Examples

This example shows how to display statistics of an access point:

```
> 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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display a list of management users:

> **show mgmtuser**

User Name	Permissions	Description	Password Strength
-----	-----	-----	-----
admin	read-write		Weak

Related Commands	config mgmtuser add config mgmtuser delete config mgmtuser description config mgmtuser password

Show 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** command.

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

Syntax Description	wlan	(Optional) Displays wireless LAN mobility group settings.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512 (inclusive).
	guest-lan	(Optional) Displays guest LAN mobility group settings.
	<i>guest_lan_id</i>	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 This example shows how to display a mobility wireless LAN anchor list:

```
> 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 foreign-map
show mobility statistics
show mobility summary

show mobility foreign-map

To display a mobility wireless LAN foreign map list, use the **show mobility foreign-map** command.

show mobility foreign-map wlan *wlan_id*

Syntax Description

wlan	Displays the mobility WLAN foreign-map list.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to get a mobility wireless LAN foreign map list:

```
> show mobility foreign-map wlan 2
```

Mobility Foreign Map List

WLAN ID	Foreign MAC Address	Interface
-----	-----	-----
2	00:1b:d4:6b:87:20	dynamic-105

Related Commands

[config wlan mobility foreign-map](#)
[config mobility group member](#)
[config wlan mobility anchor](#)
[debug mobility](#)
[show mobility anchor](#)
[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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display statistics of the mobility manager:

```
> 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

This command has no arguments or keywords.

Defaults

None.

Usage Guidelines

Some WLAN controllers may list no mobility security mode.

Examples

This example shows how to display a summary of the mobility manager:

```
> 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
```

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.

show msglog

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Usage Guidelines

If there are more than 15 entries, you are prompted to display the messages shown in the example.

Examples

This example shows how to display message logs:

```
> 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, gw 1.100.49.1
Thu Aug 4 14:29:32 2005 [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Thu Aug 4 14:29:32 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11a switch group
reset
Thu Aug 4 14:29:32 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Thu Aug 4 14:29:22 2005 [ERROR] sim.c 2841: Unable to get link state for primary port 0
of interface ap-manager
Thu Aug 4 14:29:22 2005 [ERROR] dtl_l2_dot1q.c 767: Unable to get USP
Thu Aug 4 14:29:22 2005 Previous message occurred 2 times
Thu Aug 4 14:29:14 2005 [CRITICAL] osapi_sem.c 794: Error! osapiMutexTake called with
NULL pointer: osapi_bsntime.c:927
Thu Aug 4 14:29:14 2005 [CRITICAL] osapi_sem.c 794: Error! osapiMutexTake called with
NULL pointer: osapi_bsntime.c:919
Thu Aug 4 14:29:14 2005 [CRITICAL] hwutils.c 1861: Security Module not found
Thu Aug 4 14:29:13 2005 [CRITICAL] bootos.c 791: Starting code...
```

show 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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display detailed statistics of network access control settings:

> **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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display a summary information of network access control settings:

> **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

To display the configuration of a particular user in the local user database, use **show netuser** command.

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

Syntax Description

detail	Displays detailed information about the specified network user.
<i>user_name</i>	Network user.
guest_roles	Displays configured roles for guest users.
summary	Displays a summary of all users in the local user database.

Defaults

None.

Examples

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

```
> show netuser summary
```

```
Maximum logins allowed for a given username .....Unlimited
```

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

```
> show netuser detail john10
```

```
username..... abc
WLAN Id..... Any
Lifetime..... Permanent
Description..... test user
```

Related Commands

[config netuser add](#)
[config netuser delete](#)
[config netuser description](#)
[config netuser guest-role apply](#)
[config netuser wlan-id](#)
[show netuser guest-roles](#)

show netuser guest-roles

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

show netuser guest-roles

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

```
> show netuser guest-roles

Role Name..... Contractor
  Average Data Rate..... 10
  Burst Data Rate..... 10
  Average Realtime Rate..... 100
  Burst Realtime Rate..... 100

Role Name..... Vendor
  Average Data Rate..... unconfigured
  Burst Data Rate..... unconfigured
  Average Realtime Rate..... unconfigured
  Burst Realtime Rate..... unconfigured
```

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

show network

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

show network

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the network details: > show network

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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display a summary configuration:

> **show network summary**

```
RF-Network Name..... RF
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Web Mode Cipher-Option High..... Disable
Secure Web Mode Cipher-Option SSLv2..... Disable
Secure 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 multicast group identification (MGID), use the **show network multicast mgid detail** command.

show network multicast mgid detail *mgid_value*

Syntax Description

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

Defaults

None.

Examples

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

```
> show network multicast mgid detail
```

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

Related Commands

[show network](#)
[show network summary](#)
[show network multicast mgid summary](#)

show network multicast mgid summary

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

show network multicast mgid summary

Syntax Description This command has no arguments or keywords.

Defaults None.

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

```
> show network multicast mgid summary
```

```
Layer2 MGID Mapping:
```

```
-----  
InterfaceName          vlanId    MGID  
-----  
management             0         0  
test                   0         9  
wired                  20        8
```

```
Layer3 MGID Mapping:
```

```
-----  
Number of Layer3 MGIDs ..... 1
```

```
Group address          Vlan      MGID  
-----  
239.255.255.250       0         550
```

Related Commands

- [show network](#)
- [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.

Defaults

None.

Examples

This example shows how to display NMSP configuration settings:

```
> show nmsp notify-interval summary
```

```
NMSP Notification Interval Summary
```

```
Client
  Measurement interval:    2 sec
RFID
  Measurement interval:    8 sec
Rogue AP
  Measurement interval:    2 sec
Rogue Client
  Measurement interval:    2 sec
```

Related Commands

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

show nmsp statistics

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

show nmsp statistics {summary | connection all}

Syntax Description

summary	Displays common NMSP counters.
connection all	Displays all connection-specific counters.

Defaults

None.

Examples

This example shows how to display a summary of common NMSP counters:

```
> show nmsp statistics summary

Send RSSI with no entry:          0
Send too big msg:                 0
Failed SSL write:                 0
Partial SSL write:                0
SSL write attempts to want write:
Transmit Q full:0
Max Measure Notify Msg:           0
Max Info Notify Msg:              0
Max Tx Q Size:                    2
Max Rx Size:                      1
Max Info Notify Q Size:           0

Max Client Info Notify Delay:     0
Max Rogue AP Info Notify Delay:   0
Max Rogue Client Info Notify Delay: 0
Max Client Measure Notify Delay:  0
Max Tag Measure Notify Delay:     0
Max Rogue AP Measure Notify Delay: 0
Max Rogue Client Measure Notify Delay: 0
Max Client Stats Notify Delay:    0
Max Tag Stats Notify Delay:       0
RFID Measurement Periodic :       0
RFID Measurement Immediate :      0
Reconnect Before Conn Timeout:    0
```

This example shows how to display all the connection-specific NMSP counters:

```
> show nmsp statistics connection all

NMSP Connection Counters
Connection 1 :
  Connection status:  UP
  Freed Connection:   0
  Nmsp Subscr Req:    0      Nmsp Subscr Resp:  0
  Info Req:           1      Info Resp:         1
  Measure Req:        2      Measure Resp:      2
  Stats Req:          2      Stats Resp:        2
  Info Notify:        0      Measure Notify:    0
  Loc Capability:     2
```

show nmsp statistics

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.

Defaults	None.

Examples	This example shows how to display the status of the active NMSP connections:

>show nmsp status

LocServer	IP	TxEchoResp	RxEchoReq	TxData	RxData
171.71.132.158	21642	21642	51278	21253	

Related Commands	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

summary	Displays all of the NMSP services to which the controller is subscribed.
detail	Displays details for all of the NMSP services to which the controller is subscribed.
<i>ip_addr</i>	Details only for the NMSP services subscribed to by a specific IP address.

Defaults

None.

Examples

This example shows how to display a summary of all the NMSP services to which the controller is subscribed:

```
> show nmsp subscription summary
```

Mobility Services Subscribed:

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

This example shows how to display details of all the NMSP services:

```
> show nmsp subscription detail 10.10.10.31
```

Mobility Services Subscribed by 10.10.10.31

Services	Sub-services
-----	-----
RSSI	Mobile Station, Tags,
Info	Mobile Station,
Statistics	Mobile Station, Tags,

Related Commands

[clear locp statistics](#)
[clear nmsp statistics](#)
[config nmsp notify-interval measurement](#)
[show nmsp notify-interval summary](#)
[show nmsp 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	all	Displays information about all entries in the PMK cache.
	MAC	Information about a single entry in the PMK cache.

Defaults None.

Examples This example shows how to display information about a single entry in the PMK cache:

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

This example shows how to display information about all entries in the PMK cache:

```
> 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

port	Information on the individual ports.
summary	Displays all ports.

Defaults

None.

Examples

This example shows how to display information about an individual wireless LAN controller port:

```
> 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.

This example shows how to display a summary of all ports:

```
> 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** command.

show process {cpu | memory}

Syntax Description

cpu	Displays how various system tasks are using the CPU at that moment.
memory	Displays the allocation and deallocation of memory from various processes in the system at that moment.

Defaults

None.

Usage Guidelines

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

Examples

This example shows how to display various tasks in the system that are using the CPU at a given moment:

```
> show process cpu
```

Name	Priority	CPU Use	Reaper	
reaperWatcher	(3/124)	0 %	(0/ 0)%	I
osapiReaper	(10/121)	0 %	(0/ 0)%	I
TempStatus	(255/ 1)	0 %	(0/ 0)%	I
emWeb	(255/ 1)	0 %	(0/ 0)%	T 300
cliWebTask	(255/ 1)	0 %	(0/ 0)%	I
UtilTask	(255/ 1)	0 %	(0/ 0)%	T 300

This example shows how to display the allocation and deallocation of memory from various processes at a given moment:

```
> show process memory
```

Name	Priority	BytesinUse	Reaper	
reaperWatcher	(3/124)	0	(0/ 0)%	I
osapiReaper	(10/121)	0	(0/ 0)%	I
TempStatus	(255/ 1)	308	(0/ 0)%	I
emWeb	(255/ 1)	294440	(0/ 0)%	T 300
cliWebTask	(255/ 1)	738	(0/ 0)%	I
UtilTask	(255/ 1)	308	(0/ 0)%	T 300

Related Commands

[debug memory](#)
[transfer upload datatype](#)

show qos queue_length all

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

show qos queue_length all

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display QoS queue length information:

```
> 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 queue_length](#)

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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display RADIUS accounting server statistics:

> **show radius acct statistics**

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

Related Commands

- [config radius acct](#)
- [config radius acct ipsec authentication](#)
- [config radius acct ipsec disable](#)
- [config radius acct network](#)
- [show radius auth statistics](#)
- [show radius summary](#)

show radius auth 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	This command has no arguments or keyword.

Defaults	None.

Examples	This example shows how to display RADIUS authentication server statistics:

> **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	config radius auth config radius auth management config radius auth network 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 This command has no arguments or keywords.

Defaults None.

Usage Guidelines RFC 3576, an extension to the RADIUS protocol, allows dynamic changes to a user session, which 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. CoA messages modify session authorization attributes such as data filters.

Examples This example shows how to display the RADIUS RFC-3576 server statistics:

```
> 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

- [config radius auth rfc3576](#)
- [show radius auth statistics](#)
- [show radius summary](#)

show radius summary

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

show radius summary

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display a RADIUS authentication server summary:

```
> 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 acct statistics](#)
[show radius auth statistics](#)

Show Radio Frequency ID Commands

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

show rfid client

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

show rfid client

Syntax Description This command has no arguments or keywords.

Defaults None.

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

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

```
> show rfid client
```

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

Related Commands

- [config rfid status](#)
- [config rfid timeout](#)
- [show rfid config](#)
- [show rfid detail](#)
- [show rfid summary](#)

show rfid config

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

show rfid config

Syntax Description This command has no arguments or keywords.

Defaults None.

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

> **show rfid config**

```
RFID Tag Data Collection ..... Enabled
RFID Tag Auto-Timeout ..... Enabled
RFID Client Data Collection ..... Disabled
RFID Data Timeout ..... 200 seconds
```

Related Commands

- [config rfid status](#)
- [config rfid timeout](#)
- [show rfid client](#)
- [show rfid detail](#)
- [show rfid summary](#)

show rfid detail

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

show rfid detail *mac_address*

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

Defaults	None.

Examples This example shows how to display detailed RFID information:

```
> 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 status](#)
[config rfid timeout](#)
[show rfid config](#)
[show rfid client](#)
[show rfid summary](#)

show rfid summary

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

show rfid summary

Syntax Description This command has no arguments or keywords.

Defaults None.

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

```
> show rfid summary
```

```
Total Number of RFID : 5
```

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

Related Commands

- [config rfid status](#)
- [config rfid timeout](#)
- [show rfid client](#)
- [show rfid config](#)
- [show rfid detail](#)

Show Rogue Commands

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

show rogue adhoc detailed

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

show rogue adhoc detailed *MAC*

Syntax Description	<i>MAC</i>	Ad-hoc rogue MAC address.

Defaults	None.

Examples This example shows how to display detailed ad-hoc rogue MAC address information:

```
> 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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display a summary of all ad-hoc rogues:

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

show rogue ap clients *ap_mac_address*

Syntax Description

<i>ap_mac_address</i>	Rogue access point MAC address.

Defaults

None.

Examples

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

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

show rogue ap detailed *ap_mac_address*

Syntax Description

<i>ap_mac_address</i>	Rogue access point MAC address.

Defaults

None.

Examples

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

```
> 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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display a summary of all rogue access points:

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

show rogue ap friendly summary

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display a summary of all friendly rogue access points:

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

show rogue ap malicious summary

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display a summary of all malicious rogue access points:

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

show rogue ap unclassified summary

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display a list of all unclassified rogue access points:

```
> 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 auto-contain

To display information about rogue auto-containment, use the **show rogue auto-contain** command.

show rogue auto-contain

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display information about rogue auto-containment:

```
> show rogue auto-contain
```

```
Containment Level..... 3
monitor_ap_only..... false
```

Related Commands	config rogue adhoc config rogue auto-contain level

show rogue client detailed

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

show rogue client detailed *MAC*

Syntax Description	MAC	Rogue client MAC address.

Defaults	None.

Examples This example shows how to display detailed information for a rogue client:

```
> 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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display a list of all rogue clients:

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

show rogue ignore-list

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display a list of all rogue access points that are configured to be ignored:

```
> show rogue ignore-list
```

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

Related Commands

- [config rogue adhoc](#)
- [config rogue ap classify](#)
- [config rogue ap friendly](#)
- [config rogue ap rldp](#)
- [config rogue ap ssid](#)
- [config rogue ap timeout](#)
- [config rogue ap valid-client](#)
- [config rogue 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 display detailed information for a specific rogue classification rule, use the **show rogue rule detailed** command.

show rogue rule detailed *rule_name*

Syntax Description	<i>rule_name</i>	Rogue rule name.

Defaults	None.

Examples This example shows how to display detailed information on a specific rogue classification rule:

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

show rogue rule summary

Syntax Description This command has no arguments or keywords.

Defaults None.

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

> **show rogue rule summary**

Priority	Rule Name	State	Type	Match	Hit	Count
-----	-----	-----	-----	-----	-----	-----
1	mtest	Enabled	Malicious	All	0	
2	asdfasdf	Enabled	Malicious	All	0	

Related Commands

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

show route summary

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

show route summary

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

```
> show route summary
```

```
Number of Routes..... 1
```

Destination Network	Genmask	Gateway
-----	-----	-----
xxx.xxx.xxx.xxx	255.255.255.0	xxx.xxx.xxx.xxx

Related Commands	config route

show rules

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

show rules

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display active internal firewall rules:

> **show rules**

```

-----
Rule ID.....: 3
Ref count.....: 0
Precedence.....: 99999999
Flags.....: 00000001 ( PASS )
Source IP range:
    (Local stack)
Destination IP range:
    (Local stack)
-----
Rule ID.....: 25
Ref count.....: 0
Precedence.....: 99999999
Flags.....: 00000001 ( PASS )
Service Info
    Service name.....: GDB
    Protocol.....: 6
    Source port low.....: 0
    Source port high.....: 0
    Dest port low.....: 1000
    Dest port high.....: 1000
Source IP range:
IP High.....: 0.0.0.0
    Interface.....: ANY
Destination IP range:
    (Local stack)
-----

```

show run-config

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

show run-config [**no ap** | **commands**]

Syntax Description

no-ap	(Optional) Excludes access point configuration settings.
commands	(Optional) Displays a list of user-configured commands on the controller.

Defaults

None.

Usage Guidelines

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

Some WLAN controllers may have no Crypto Accelerator (VPN termination module) or power supplies listed because they have no provisions for VPN termination modules or power supplies.

The **show run-config** command shows only values configured by the user. It does not show system-configured default values.

Examples

This example shows how to display the current controller running configuration:

```
> show run-config
```

```
Press Enter to continue...
```

```
System Inventory
Switch Description..... Cisco Controller
Machine Model.....
Serial Number..... FLS0923003B
Burned-in MAC Address..... xx:xx:xx:xx:xx:xx
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK
```

```
Press Enter to continue Or <Ctl Z> to abort...
```

Related Commands

[config passwd-cleartext](#)

show serial

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

show serial

Syntax Description	This command has no arguments or keywords.

Defaults	9600, 8, off, 1, none.

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

> **show serial**

```
Serial Port Login Timeout (minutes)..... 45
Baud Rate..... 9600
Character Size..... 8
Flow Control:..... Disable
Stop Bits..... 1
Parity Type:..... none
```

Related Commands	config serial baudrate config serial timeout

show sessions

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

show sessions

Syntax Description	This command has no arguments or keywords.

Defaults	5 minutes, 5 sessions.

Examples	This example shows how to display the CLI session configuration setting:

```
> show sessions
```

```
CLI Login Timeout (minutes)..... 0
Maximum Number of CLI Sessions..... 5
```

The response indicates that the CLI sessions never time out and that the Cisco wireless LAN controller can host up to five simultaneous CLI sessions.

Related Commands	config sessions maxsessions config sessions timeout

show snmpcommunity

To display Simple Network Management Protocol (SNMP) community entries, use the **show snmpcommunity** command.

show snmpcommunity

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display SNMP community entries:

> **show snmpcommunity**

SNMP Community Name	Client IP Address	Client IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read Only	Enable
*****	0.0.0.0	0.0.0.0	Read/Write	Enable

Related Commands

- [config snmp community accessmode](#)
- [config snmp community create](#)
- [config snmp community delete](#)
- [config snmp community ipaddr](#)
- [config snmp community mode](#)
- [config snmp syscontact](#)

show snmpengineID

To display the SNMP engine ID, use the **show snmpengineID** command.

show snmpengineID

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

```
> show snmpengineID
```

```
SNMP EngineId... ffffffff
```

Related Commands	config snmp engineID

show snmptrap

To display Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap receivers and their status, use the **show snmptrap** command.

show snmptrap

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display SNMP trap receivers and their status:

> **show snmptrap**

SNMP Trap Receiver Name	IP Address	Status
-----	-----	-----
xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	Enable

Related Commands

- [config snmp trapreceiver create](#)
- [config snmp trapreceiver delete](#)
- [config snmp trapreceiver delete](#)

show snmpv3user

To display Simple Network Management Protocol (SNMP) version 3 configuration, use the **show snmpv3user** command.

show snmpv3user

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display SNMP version 3 configuration information:

> **show snmpv3user**

SNMP v3 username	AccessMode	Authentication	Encryption
-----	-----	-----	-----
default	Read/Write	HMAC-SHA	CFB-AES

Related Commands	config snmp v3user create config snmp v3user delete

show snmpversion

To display which versions of Simple Network Management Protocol (SNMP) are enabled or disabled on your controller, use the **show snmpversion** command.

show snmpversion

Syntax Description This command has no arguments or keywords.

Defaults Enable.

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

> **show snmpversion**

```
SNMP v1  Mode..... Disable
SNMP v2c Mode..... Enable
SNMP v3  Mode..... Enable
```

Related Commands [config snmp version](#)

show spanningtree port

To display the Cisco wireless LAN controller spanning tree port configuration, use the **show spanningtree port** command.

show spanningtree port *port*

Syntax Description

port

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, the Spanning Tree Protocol (STP) must be disabled for all ports on the Cisco 4400 Series Wireless LAN Controller. STP 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

This example shows how to display spanning tree values on a per port basis:

```
> 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 mode](#)
[config spanningtree port pathcost](#)
[config spanningtree port priority](#)
[show spanningtree switch](#)

show spanningtree switch

To display the Cisco wireless LAN controller network (DS port) spanning tree configuration, use the **show spanningtree switch** command.

show spanningtree switch

Syntax Description This command has no arguments or keywords.

Defaults None.

Usage Guidelines Some WLAN controllers do not support the spanning tree function.

Examples This example shows how to display spanning tree values on a per switch basis:

```
> 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 display physical port receive and transmit statistics, use the **show stats port** command.

show stats port {*detailed port* | *summary port*}

Syntax Description		
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.

Defaults None.

Examples This example shows how to display the port summary information:

```
> 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
```

This example shows how to display the detailed port information:

```
> 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
```

■ show stats port

```

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](#)
[config port autoneg](#)
[config port linktrap](#)
[config port power](#)
[config port linktrap](#)

show stats switch

To display the network (DS port) receive and transmit statistics, use the **show stats switch** command.

show stats switch {detailed | summary}

Syntax Description	detailed	Displays detailed switch statistics.
	summary	Displays switch summary statistics.

Defaults None.

Examples This example shows how to display switch summary statistics:

```
> 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
```

This example shows how to display detailed switch statistics:

```
> 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	This command has no arguments or keywords.

Defaults	Enabled.

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

```
> show switchconfig
```

```
802.3x Flow Control Mode..... Disabled
FIPS prerequisite features..... Enabled
Boot Break..... Enabled
secret obfuscation..... Enabled
```

```
Strong Password Check Features:
  case-check .....Disabled
  consecutive-check ....Disabled
  default-check .....Disabled
  username-check .....Disabled
```

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

show sysinfo

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

show sysinfo

Syntax Description This command has no arguments or keywords.

Defaults None.

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

> **show sysinfo**

```

Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 6.0.133.0
Build Information..... Tue Mar 31 11:44:12 PDT 2009
Bootloader Version..... 0.14.0
Field Recovery Image Version..... 5.3.38.0-BL-9-16
Firmware Version..... FPGA 1.0, Env 0.8, USB console 1.27
Build Type..... DATA + WPS

System Name..... 5500
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.9.1.1
IP Address..... 10.10.10.7
Last Reset..... Software reset
System Up Time..... 1 days 15 hrs 17 mins 48 secs
System Timezone Location.....
Current Boot License Level..... wplus
Current Boot License Type..... Permanent
Next Boot License Level..... wplus
Next Boot License Type..... Permanent
Configured Country..... US - United States
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +45 C
External Temperature..... +29 C
Fan Status..... OK

State of 802.11b Network..... Enabled
State of 802.11a Network..... Disabled
Number of WLANs..... 18
3rd Party Access Point Support..... Disabled
Number of Active Clients..... 1

Burned-in MAC Address..... 00:00:1B:EE:12:E0
Power Supply 1..... Not Available
Power Supply 2..... Not Available
Maximum number of APs supported..... 250

```

Related Commands [config sysname](#)

Show TACACS Commands

Use the **show tacacs** commands to display Terminal Access Controller Access Control System (TACACS) protocol settings and statistics.

show ntp-keys

To display network time protocol authentication key details, use the **show ntp-keys** command.

show ntp-keys

Syntax Description This command has no arguments or keywords.

Defaults None.

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

```
> show ntp-keys
```

```
Ntp Authentication Key Details.....
```

```
Key Index
-----
  1
  3
```

Related Commands [config time ntp](#)

show tacacs acct statistics

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

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display detailed RFID information:

```
> 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 acct config tacacs acct config tacacs athr config tacacs auth show tacacs summary show tacacs summary

show tacacs athr statistics

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

show tacacs athr statistics

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display TACACS server authorization statistics:

```
> show tacacs athr statistics
```

```
Authorization Servers:
```

```

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

Related Commands

- [config tacacs acct](#)
- [config tacacs acct](#)
- [config tacacs athr](#)
- [config tacacs auth](#)
- [show tacacs summary](#)
- [show tacacs auth statistics](#)
- [show tacacs summary](#)

show tacacs auth statistics

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

show tacacs auth statistics

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display TACACS server authentication statistics:

```
> 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 acct config tacacs acct config tacacs athr config tacacs auth show tacacs summary show tacacs summary

show tacacs summary

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

show tacacs summary

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display TACACS server summary information:

```
> 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 acct](#)
- [config tacacs acct](#)
- [config tacacs athr](#)
- [config tacacs auth](#)
- [show tacacs summary](#)
- [show tacacs athr statistics](#)
- [show tacacs auth statistics](#)

show tech-support

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support** command.

show tech-support

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display system resource information:

```
> show tech-support

Current CPU Load..... 0%

System Buffers
  Max Free Buffers..... 4608
  Free Buffers..... 4604
  Buffers In Use..... 4

Web Server Resources
  Descriptors Allocated..... 152
  Descriptors Used..... 3
  Segments Allocated..... 152
  Segments Used..... 3

System Resources
  Uptime..... 747040 Secs
  Total Ram..... 127552 Kbytes
  Free Ram..... 19540 Kbytes
  Shared Ram..... 0 Kbytes
  Buffer Ram..... 460 Kbytes
```

show time

To display the Cisco wireless LAN controller time and date, use the **show time** command.

show time

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples When Authentication is not enabled, the output is as follows:

```
> show time

Time..... Wed Apr 13 09:29:15 2011

Timezone delta..... 0:0
Timezone location..... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata

NTP Servers
  NTP Polling Interval..... 3600

  Index      NTP Key Index      NTP Server      NTP Msg Auth Status
  -----
    1          0          9.2.60.60      AUTH DISABLED
```

A successful authentication of NTP Message results in the AUTH Success as follows:

```
> show time

Time..... Thu Apr 7 13:56:37 2011
Timezone delta..... 0:0
Timezone location..... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata

NTP Servers
  NTP Polling Interval..... 3600

  Index      NTP Key Index      NTP Server      NTP Msg Auth Status
  -----
    1          1          9.2.60.60      AUTH SUCCESS
```

If the packet received has errors, then the NTP Msg Auth status will show AUTH Failure as follows:

```
> show time

Time..... Thu Apr 7 13:56:37 2011
Timezone delta..... 0:0
Timezone location..... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata

NTP Servers
  NTP Polling Interval..... 3600

  Index      NTP Key Index      NTP Server      NTP Msg Auth Status
  -----
    1          10          9.2.60.60      AUTH FAILURE
```

If there is no response from NTP server for the packets, the NTP Msg Auth status will be blank as follows;

> **show time**

```
Time..... Thu Apr  7 13:56:37 2011
Timezone delta..... 0:0
Timezone location..... (GMT +5:30) Colombo, New Delhi, Chennai,
Kolkata
```

NTP Servers

```
NTP Polling Interval..... 3600
```

Index	NTP Key Index	NTP Server	NTP Msg Auth Status
1	11	9.2.60.60	

Related Commands

[config time manual](#)
[config time ntp](#)
[config time timezone](#)
[config time timezone location](#)
[config time timezone location](#)

show trapflags

To display the Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap flags, use the **show trapflags** command.

show trapflags

Syntax Description

This command has no arguments and keywords.

Defaults

None.

Examples

This example shows how to display controller SNMP trap flags:

```
> show trapflags
```

```
Authentication Flag..... Enable
Link Up/Down Flag..... Enable
Multiple Users Flag..... Enable
Spanning Tree Flag..... Enable

Client Related Traps
  802.11 Disassociation..... Disable
  802.11 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 802.11-Security](#)
[config trapflags aaa](#)
[config trapflags ap](#)
[config trapflags authentication](#)
[config trapflags client](#)
[config trapflags configsave](#)
[config trapflags IPsec](#)
[config trapflags linkmode](#)

show traplog

To display the Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap log, use the **show traplog** command.

show traplog

Syntax Description

This command has no arguments and keywords.

Defaults

None.

Examples

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

```
> show traplog
```

```
Number of Traps Since Last Reset..... 2447
Number of Traps Since Log Last Displayed... 2447
```

Log	System Time	Trap
0	Thu Aug 4 19:54:14 2005	Rogue AP : 00:0b:85:52:62:fe detected on Base Radio 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 Radio 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 Radio 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 Radio 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

To display access point's software information, use the **show version** command.

show version

Syntax Description	This command has no arguments or keywords.
Defaults	None.
Usage Guidelines	You can only use this command from the access point console port when not connected to a controller.
Examples	This example shows how to display the access point version number:

```
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)
Apl242-2 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
```

show watchlist

To display the client watchlist, use the **show watchlist** command.

show watchlist

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display the client watchlist information: <pre>> show watchlist client watchlist state is disabled</pre>

Related Commands	config watchlist add config watchlist delete config watchlist disable config watchlist enable

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	apgroups	(Optional) Displays access point group information.
	summary	(Optional) Displays a summary of all wireless LANs.
	<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
	foreignAp	(Optional) Displays the configuration for support of foreign access points.

Defaults None.

Examples This example shows how to display a summary of wireless LANs for wlan_id 1:

```
> show wlan 1
WLAN Identifier..... 1
Profile Name..... aicha
Network Name (SSID)..... aicha
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Admission Control

    Radius-NAC State..... Enabled
    SNMP-NAC State..... Enabled
Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
CHD per WLAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... management
Multicast Interface..... Not Configured
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Static IP client tunneling..... Enabled
Quality of Service..... Silver (best effort)
Scan Defer Priority..... 4,5,6
Scan Defer Time..... 100 milliseconds
WMM..... Allowed
Media Stream Multicast-direct..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Peer-to-Peer Blocking Action..... Disabled
Radio Policy..... All
```

■ show wlan

```

DTIM period for 802.11a radio..... 1
DTIM period for 802.11b radio..... 1
Radius Servers
  Authentication..... Global Servers
  Accounting..... Global Servers
  Dynamic Interface..... Disabled
Local EAP Authentication..... Enabled (Profile 'Controller_Local_EAP')
Security

  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Enabled
      TKIP Cipher..... Disabled
      AES Cipher..... Enabled
    WPA2 (RSN IE)..... Enabled
      TKIP Cipher..... Disabled
      AES Cipher..... Enabled
                                Auth Key Management
    802.1x..... Enabled
    PSK..... Disabled
    CCKM..... Enabled
    FT(802.11r)..... Disabled
    FT-PSK(802.11r)..... Disabled
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
  H-REAP Local Switching..... Enabled
  H-REAP Local Authentication..... Enabled
  H-REAP Learn IP Address..... Enabled
  Client MFP..... Optional
  Tkip MIC Countermeasure Hold-down Timer..... 60
Call Snooping..... Disabled
Roamed Call Re-Anchor Policy..... Disabled
Band Select..... Disabled
Load Balancing..... Disabled

Mobility Anchor List
WLAN ID      IP Address      Status
-----

```

This example shows how to display a summary of all WLANs:

```
> show wlan summary
```

```

Number of WLANs..... 2

WLAN ID  WLAN Profile Name / SSID      Status      Interface Name
-----
1         test / test                      Enabled management

```

This example shows how to display the configuration for support of foreign access points:

```
> show wlan foreignap
```

Foreign AP support is not enabled.

Related Commands

[config wlan](#)
[config wlan 7920-support](#)
[config wlan acl](#)
[config wlan interface](#)
[config wlan roamed-voice-client re-anchor](#)
[show wlan](#)

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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to display a summary of the Wireless Protection System (WPS) access point neighbor authentication:

```
> 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 System (WPS) IDS sensor, use the **show wps cids-sensor** command.

show wps cids-sensor {**summary** | **detail** *index*}

Syntax Description

summary	Displays a summary of sensor settings.
detail	Displays all settings for the selected sensor.
<i>index</i>	IDS sensor identifier.

Defaults

None.

Examples

This example shows how to display all settings for the selected sensor:

```
> 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
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	summary	Displays the MFP configuration and status.
	statistics	Displays MFP statistics.

Defaults None.

Examples This example shows how to display a summary of the MFP configuration and status:

```
> 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 a	Down Down	Full Full	Full Full

This example shows how to display the MFP statistics:

```
> 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 the 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.

Defaults None.

Examples This example shows how to display the IDS system sensor shun list:

```
> show wps shun-list
```

Related Commands [config wps shun-list re-sync](#)

show wps signature detail

To display installed signatures, use the **show wps signature detail** command.

show wps signature detail *sig-id*

Syntax Description	<i>sig-id</i> Signature ID of an installed signature.

Defaults	None.

Examples This example shows how to display information on the attacks detected by standard signature 1:

```
> 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 about 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

summary	Displays all tracking signature summary information.
standard	Displays Standard Intrusion Detection System (IDS) signature settings.
custom	Displays custom IDS signature settings.
<i>precedenceID</i>	Signature precedence identification value.
detailed	Displays tracking source MAC address details.

Defaults

None.

Examples

This example shows how to display the number of attacks detected by all enabled signatures:

```
> show wps signature events summary
```

Precedence	Signature Name	Type	# Events
1	Bcast deauth	Standard	2
2	NULN probe resp 1	Standard	1

This example shows how to display a summary of information on the attacks detected by standard signature 1:

```
> 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.

Defaults	None.

Examples	This example shows how to display a summary of all of the standard and custom signatures:

```
> 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 Wireless Protection System (WPS) summary information, use the **show wps summary** command.

show wps summary

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display WPS summary information:

```
> 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 the Cisco Wireless Intrusion Prevention System (wIPS) operation on the controller, use the **show wps wips statistics** command.

show wps wips statistics

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to display the statistics of the wIPS operation:

```
> 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 the adaptive Cisco Wireless Intrusion Prevention System (wIPS) configuration that the Wireless Control System (WCS) forwards to the controller, use the **show wps wips summary** command.

show wps wips summary

Syntax Description	This command has no arguments or keywords.

Defaults	None.

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

```
> 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 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a** commands.

```
config {802.11-a49 | 802.11-a58} {enable | disable} cisco_ap
```

Syntax Description	802.11-a49	Specifies the 4.9-GHz public safety channel.
	802.11-a58	Specifies the 5.8-GHz public safety channel.
	enable	Enables the use of this frequency on the designated access point.
	disable	Disables the use of this frequency on the designated access point.
	<i>cisco_ap</i>	Name of the access point to which the command applies.

Defaults	Disabled.

Examples	This example shows how to enable the 4.9-GHz public safety channel on <i>ap_24</i> access point: <pre>> config 802.11-a49 enable ap_24</pre>

Related Commands	config 802.11-a antenna extAntGain config 802.11-a channel ap config 802.11-a txpower ap show mesh public-safety

config 802.11-a antenna extAntGain

To configure the external antenna gain for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a antenna extAntGain** commands.

```
config {802.11-a49 | 802.11-a58} antenna extAntGain ant_gain cisco_ap {global | channel_no}
```

Syntax Description	802.11-a49	Specifies the 4.9-GHz public safety channel.
	802.11-a58	Specifies the 5.8-GHz public safety channel.
	<i>ant_gain</i>	Value in .5-dBi units (for instance, 2.5 dBi = 5).
	<i>cisco_ap</i>	Name of the access point to which the command applies.
	global	Specifies the antenna gain value to all channels.
	<i>channel_no</i>	Antenna gain value for a specific channel.

Defaults 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 This example shows how to configure an *802.11-a49* external antenna gain of *10 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 Commands](#)

config 802.11-a channel ap

To configure the channel properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a channel ap** command.

```
config {802.11-a49 | 802.11-a58} channel ap cisco_ap {global | channel_no}
```

Syntax Description	802.11-a49	Specifies the 4.9-GHz public safety channel.
	802.11-a58	Specifies the 5.8-GHz public safety channel.
	<i>cisco_ap</i>	Name of the access point to which the command applies.
	global	Enables the Dynamic Channel Assignment (DCA) on all 4.9-GHz and 5.8-GHz subband radios.
	<i>channel_no</i>	Custom channel for a specific mesh access point. The range is 1 through 26, inclusive, for a 4.9-GHz band and 149 through 165, inclusive, for a 5.8-GHz band.

Defaults	Disabled.

Examples	This example shows how to set the channel properties:

```
> 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

config 802.11-a txpower ap

To configure the transmission power properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a txpower ap** command.

```
config {802.11-a49 | 802.11-a58} txpower ap cisco_ap {global | power_level}
```

Syntax Description	802.11-a49	Specifies the 4.9-GHz public safety channel.
	802.11-a58	Specifies the 5.8-GHz public safety channel.
	txpower	Configures transmission power properties.
	ap	Configures access point channel settings.
	cisco_ap	Name of the access point to which the command applies.
	global	Applies the transmission power value to all channels.
	power_level	Transmission power value to the designated mesh access point. Valid values are 1 through 5, inclusive.

Defaults Disabled.

Examples This example shows how 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 Commands](#)

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}

Syntax Description

enable	Enables the 802.11g network.
disable	Disables the 802.11g network.

Defaults

Enabled.

Usage Guidelines

Before you enter the **config 802.11b 11gSupport {enable | disable}** command, disable the 802.11 Cisco radio with the **config 802.11 disable** command.

After you configure the support for the 802.11g network, use the **config 802.11 enable** command to enable the 802.11 radio.



Note

To disable an 802.11a, 802.11b and/or 802.11g network for an individual wireless LAN, use the **config wlan radio** command.

Examples

This example shows how to enable the 802.11g network:

```
> 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

long	Specifies the long 802.11b preamble.
short	Specifies the 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 that the CLI interface is active.

Examples

This example shows how to change the 802.11b preamble to short:

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

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

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

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

Defaults	None.

Examples	This example shows how to disable the 802.11h switch announcement: <pre>> config 802.11h channelswitch disable</pre>

Related Commands	show 802.11h

config 802.11h powerconstraint

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

config 802.11h powerconstraint *value*

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

Defaults	None.

Examples	This example shows how to configure the 802.11h power constraint to 5: > config 802.11h powerconstraint 5

Related Commands	show 802.11h

config 802.11h setchannel

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

config 802.11h setchannel *cisco_ap*

Syntax Description

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

Defaults

None.

Examples

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

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

Related Commands

show 802.11h

Configure 802.11 11n Support Commands

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

Defaults None.

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

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

Related Commands

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

config 802.11 11nsupport a-mpdu tx priority

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

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

Syntax Description

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

Defaults

All priorities, except 5 and 6, are enabled by default. Priorities 5 and 6 are disabled by default.

Usage Guidelines

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

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

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



Note

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

Examples

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

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

Related Commands

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

config 802.11 11nsupport 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
tx	Enables the antenna to transmit.
rx	Enables the antenna to receive.
<i>cisco_ap</i>	Access point.
A	Specifies the right antenna port.
B	Specifies the left antenna port.
C	Specifies the center antenna port.
enable	Enables the configuration.
disable	Disables the configuration.

Defaults

None.

Examples

This example shows how to configure access point AP1 to use the antenna tx to transmit:

```
> 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 11nsupport mcs tx

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

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

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

Defaults None.

Examples This example shows how to specify MCS rates:

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

Related Commands

```
config 802.11 11nsupport
config wlan wmm required
config 802.11 11nsupport a-mpdu tx priority
```

```
config 802.11a disable network
config 802.11a disable
config 802.11a channel ap
config 802.11a txpower ap
config 802.11a chan_width
```

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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the diversity.
sideA	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point left port.
sideB	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point right port.
<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults

None.

Examples

This example shows how to enable antenna diversity for AP01 on an 802.11b network:

```
> config 802.11b antenna diversity enable AP01
```

This example shows how to enable diversity for AP01 on an 802.11a network, using an external antenna connected to the Cisco lightweight access point left port (sideA):

```
> 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 Commands](#)

config 802.11 antenna extAntGain

To configure external antenna gain for an 802.11 network, use the **config 802.11 antenna extAntGain** command.

config 802.11{a | b} antenna extAntGain antenna_gain cisco_ap

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
<i>antenna_gain</i>	Antenna gain in 0.5 dBm units (for example, 2.5 dBm = 5).
<i>cisco_ap</i>	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

This example shows how 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 Commands](#)

config 802.11 antenna mode

To configure the Cisco lightweight access point to use one internal antenna for an 802.11 sectorized 180-degree coverage pattern or both internal antennas for an 802.11 360-degree omnidirectional pattern, use the **config 802.11 antenna mode** command.

config 802.11 {a | b} antenna mode {omni | sectorA | sectorB} cisco_ap

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	omni	Specifies to use both internal antennas.
	sectorA	Specifies to use only the side A internal antenna.
	sectorB	Specifies to use only the side B internal antenna.
	<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults None.

Examples This example shows how to configure access point AP01 antennas for a 360-degree omnidirectional pattern on an 802.11b network:

```
> 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 Commands](#)

config 802.11 antenna selection

To select the internal or external antenna selection for a Cisco lightweight access point on an 802.11 network, use the **config 802.11 antenna selection** command.

config 802.11{a | b} antenna selection {internal | external} *cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
internal	Specifies the internal antenna
external	Specifies the external antenna.
<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults

None.

Examples

This example shows how to configure access point AP02 on an 802.11b network to use the internal antenna:

```
> 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 Commands](#)

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 the “Usage Guidelines” section.

Syntax Description

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

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 the 802.11a service is available and allows the clients to synchronize with the lightweight access point.

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

Examples

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

```
> config 802.11a 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}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Specifies all lightweight access points.
ap <i>ap_name</i>	Specifies the Cisco access point name.
enable	Enables beamforming.
disable	Disables beamforming.

Defaults

None.

Usage Guidelines

When you enable beamforming on the network, it is automatically enabled for all the radios applicable to that network type.

Follow these guidelines for using beamforming:

- Beamforming is supported only for legacy orthogonal frequency-division multiplexing (OFDM) data rates (6, 9, 12, 18, 24, 36, 48, and 54 mbps).



Note Beamforming is not supported for complementary-code keying (CCK) data rates (1, 2, 5.5, and 11 Mbps).

- Beamforming is supported only on access points that support 802.11n (AP1250 and AP1140).
- Two or more antennas must be enabled for transmission.
- All three antennas must be enabled for reception.
- OFDM rates must be enabled.

If the antenna configuration restricts operation to a single transmit antenna, or if OFDM rates are disabled, beamforming is not used.

Examples

This example shows how to enable beamforming on the 802.11a network:

```
> config 802.11a beamforming global enable
```

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 CleanAir Commands

Use the **config 802.11 cleanair** commands to configure cleanair settings on different 802.11 networks.

config 802.11 cleanair

To enable or disable cleanair for the 802.11 a or 802.11 b/g network, use the **config 802.11 cleanair** command.

config 802.11 cleanair {enable | disable} {network | cisco_ap}

enable	Enables the cleanair settings.
disable	Disables the cleanair settings.
network	Configures all 5-GHz Cisco APs.
cisco_ap	Name of the access point to which the command applies.

Defaults

Disabled.

Examples

This example shows how to enable the cleanair settings on access point ap_24:

```
> config 802.11a cleanair enable ap_24
```

Related Commands

config 802.11 cleanair device

config 802.11 cleanair device

To configure cleanair interference device types, use the **config 802.11 cleanair device** command.

config 802.11a cleanair device {enable | disable} device_type

Syntax Description	enable	Enables the CleanAir reporting for the interference device type.
	disable	Disables the CleanAir reporting for the interference device type.
	reporting	Configures CleanAir interference device reporting.
	device_type	Interference device type. The device type are as follows: • 802.11-nonstd—Devices using nonstandard WiFi channels. • 802.11-inv—Devices using spectrally inverted WiFi signals. • superag—802.11 SuperAG devices. • all —All interference device types. • cont-tx—Continuous Transmitter. • dect-like—Digital Enhanced Cordless Communication (DECT) like phone. • tdd-tx—TDD Transmitter. • jammer—Jammer. • canopy—Canopy devices. • video—Video cameras. • wimax-mobile—WiMax Mobile. • wimax-fixed—WiMax Fixed.

Defaults Disabled.

Examples This example shows how to enable the CleanAir reporting for the device type jammer:

```
> config 802.11a cleanair device enable jammer
```

This example shows how to disable the CleanAir reporting for the device type video:

```
> config 802.11a cleanair device disable video
```

This example shows how to enable the CleanAir interference device reporting:

```
> config 802.11a cleanair device reporting enable
```

Related Commands config 802.11 cleanair

config 802.11 cleanair alarm

To configure the triggering of the air quality alarms, use the **config 802.11 cleanair alarm** command.

config 802.11 cleanair alarm

{air-quality {disable | enable | threshold *threshold*}}

device {disable [*device_type* | all] | enable [*device_type* | all] | reporting [enable | disable]}

Syntax Description

air-quality	Configures the 5-GHz air quality alarm.
device	Configures the 5-GHz cleanair interference devices alarm.
disable	Disables the 5-GHz air quality alarm.
enable	Enables the 5-GHz air quality alarm.
threshold	Configure the 5-GHz air quality alarm threshold.
disable	Disables the 5-GHz CleanAir alarm for the interference device type.
enable	Enables the 5-GHz CleanAir alarm for the interference device type.
reporting	Configures the 5-GHz CleanAir interference devices alarm reporting.
<i>threshold</i>	Air quality alarm threshold (1 is bad air quality, and 100 is good air quality).
<i>device_type</i>	Device types. The device types are as follows: • 802.11-nonstd—Devices using nonstandard WiFi channels. • 802.11-inv—Devices using spectrally inverted WiFi signals. • superag—802.11 SuperAG devices. • all —All interference device types. • cont-tx—Continuous Transmitter. • dect-like—Digital Enhanced Cordless Communication (DECT) like phone. • tdd-tx—TDD Transmitter. • jammer—Jammer. • canopy—Canopy devices. • video—Video cameras. • wimax-mobile—WiMax Mobile. • wimax-fixed—WiMax Fixed.
all	Configures all the device types at once.

Defaults

Enabled.

Examples

This example shows how to enable the CleanAir alarm to monitor the air quality:

```
> config 802.11a cleanair alarm air-quality enable
```

This example shows how to enable the CleanAir alarm for the device type video:

```
> config 802.11a cleanair alarm device enable video
```

This example shows how to enable alarm reporting for the CleanAir interference devices:

```
> config 802.11a cleanair alarm device reporting enable
```

Related Commands config 802.11 cleanair

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

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

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

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

Examples

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

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

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

```
> 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

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

Defaults

0%.

Usage Guidelines

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



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

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

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

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

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

Examples

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

```
> config 802.11a cac video max-bandwidth 50
```

Related Commands

[config 802.11 cac video acm](#)
[config 802.11 cac video roam-bandwidth](#)
[config 802.11 cac voice stream-size](#)
[config 802.11 cac voice roam-bandwidth](#)

config 802.11 cac video roam-bandwidth

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

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

Syntax Description

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

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

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

Examples

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

```
> config 802.11a cac video roam-bandwidth 10
```

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

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

Syntax Description

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

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

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

Examples

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

```
> config 802.11a cac video tspec-inactivity-timeout enable
```

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

```
> config 802.11b 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

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

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

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

Examples

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

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

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

```
> config 802.11b cac voice acm disable
```

Related Commands

[config 802.11 cac video acm](#)

config 802.11 cac voice max-bandwidth

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

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

Syntax Description

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

Defaults

0%.

Usage Guidelines

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

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

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

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

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

Examples

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

```
> config 802.11a cac voice max-bandwidth 50
```

Related Commands

```
config 802.11 cac voice 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
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

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

Defaults

85%.

Usage Guidelines

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



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

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

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

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

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

Examples

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

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

Related Commands

config 802.11 cac voice acm
config 802.11 cac voice max-bandwidth
config 802.11 cac voice stream-size

config 802.11 cac voice tspec-inactivity-timeout

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

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

Syntax Description

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

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

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

Examples

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

```
> config 802.11a cac voice tspec-inactivity-timeout enable
```

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

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

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

Syntax Description

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

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

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

Examples

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

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

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

```
> config 802.11b 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 max-calls

**Note**

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

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

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

Syntax Description

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

Defaults

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

Usage Guidelines

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

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

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

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

Examples

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

```
> config 802.11a cac voice max-calls 10
```

Related Commands

config 802.11 cac voice acm
config 802.11 cac voice load-based
config 802.11 cac voice max-bandwidth
config 802.11 cac voice roam-bandwidth
config 802.11 cac voice tspec-inactivity-timeout
config 802.11 exp-bwreq

■ config 802.11 cac voice max-calls

config 802.11 cac voice sip bandwidth

**Note**

SIP bandwidth and sample intervals are used to compute per call bandwidth in case of the SIP based CAC.

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

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

Syntax Description

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

Defaults

None.

Usage Guidelines

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

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

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

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

Examples

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

```
> config 802.11a cac voice sip bandwidth 10 sample-interval 40
```

Related Commands

config 802.11 cac voice acm
config 802.11 cac voice load-based
config 802.11 cac voice max-bandwidth
config 802.11 cac voice roam-bandwidth
config 802.11 cac voice tspec-inactivity-timeout
config 802.11 exp-bwreq

config 802.11 cac voice sip codec

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

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

Syntax Description

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

Defaults

g711.

Usage Guidelines

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

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

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

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

Examples

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

```
> config 802.11a cac voice sip codec g729 sample-interval 40
```

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

```
> config 802.11b cac voice sip codec 9711 sample-interval 10
```

Related Commands

config 802.11 cac voice acm
config 802.11 cac voice load-based
config 802.11 cac voice max-bandwidth
config 802.11 cac voice roam-bandwidth
config 802.11 cac voice tspec-inactivity-timeout
config 802.11 exp-bwreq

config 802.11 cac voice stream-size

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

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

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

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

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

Examples

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

```
> config 802.11a cac voice stream-size 5 max-streams size 85
```

Related Commands

config 802.11 cac voice acm
config 802.11 cac voice load-based
config 802.11 cac voice max-bandwidth
config 802.11 cac voice roam-bandwidth
config 802.11 cac voice tspec-inactivity-timeout
config 802.11 exp-bwreq

config 802.11 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
auto	(Optional) Specifies that the channel is automatically set by Radio Resource Management (RRM) for the 802.11a radio.
once	(Optional) Specifies that the channel is automatically set once by RRM.
off	(Optional) Specifies that the automatic channel selection by RRM is disabled.
<i>ap_name</i>	Access point name.
global	Specifies the 802.11a operating channel that is automatically set by RRM and overrides the existing configuration setting.
<i>channel</i>	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, enter the **config 802.11 disable** command to disable the 802.11 network. Enter the **config 802.11 channel** command to set automatic channel selection by Radio Resource Management (RRM) or manually set the channel for the 802.11 radio, and enter the **config 802.11 enable** command to enable the 802.11 network.



Note See the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the channels supported by your access point. The power levels and available channels are defined by the country code setting and are regulated on a country-by-country basis.

Examples

This example shows how to have RRM automatically configure the 802.11a channels for automatic channel configuration based on the availability and interference:

```
> config 802.11a channel global auto
```

This example shows how to configure the 802.11b channels one time based on the availability and interference:

```
> config 802.11b channel global once
```

This example shows how to turn 802.11a automatic channel configuration off:

```
> config 802.11a channel global off
```

This example shows how to configure the 802.11b channels in access point AP01 for automatic channel configuration:

```
> config 802.11b channel AP01 global
```

This example shows how to configure the 802.11a channel 36 in access point AP01 as the default channel:

```
> 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	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	<i>cisco_ap</i>	Name of the Cisco access point.
	global	Enables auto-RF on the designated access point.
	<i>channel_no</i>	Default channel from 1 to 26, inclusive.

Defaults	None.

Examples	This example shows how to enable auto-RF for access point AP01 on an 802.11b network: <pre>> config 802.11b channel ap ap01 global</pre>

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, use the **config 802.11 chan_width** command.

```
config 802.11 {a | b} chan_width cisco_ap {20 | 40}
```

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
<i>cisco_ap</i>	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

The default channel width is **20**.

Usage Guidelines

This parameter can be configured only if the primary channel is statically assigned.



Caution

We recommend that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference can occur.

Statically configuring an access point's radio for 20- or 40-MHz mode overrides the globally configured DCA channel width setting (configured by using the [config advanced 802.11 channel dca chan-width-11n](#) command). If you change the static configuration back to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

Examples

This example shows how to configure the channel width for access point AP01 on an 802.11 network using 40-MHz channels:

```
> config 802.11a chan_width AP01 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

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

Defaults

The transmission is enabled for the entire network by default.



Usage Guidelines

Note You must use this command to disable the network before using many config 802.11 commands.

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

Examples

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

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

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

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

Related Commands

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


config 802.11 dtpc

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

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

Syntax Description

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

Defaults

Enabled.

Examples

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

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

Related Commands

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

config 802.11 enable

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

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

Syntax Description

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

Defaults

The transmission is enabled for the entire network by default.

Usage Guidelines



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

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

Examples

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

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

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

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

Related Commands

```
show sysinfo
show 802.11a
config wlan radio
config 802.11a disable
config 802.11b disable
config 802.11b enable
config 802.11b 11gSupport enable
config 802.11b 11gSupport disable
```

config 802.11 exp-bwreq

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

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

Syntax Description

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

Defaults

The expedited bandwidth request feature is disabled by default.

Usage Guidelines

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

Examples

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

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

```
Cannot change Exp Bw Req mode while 802.11a network is operational.
```

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

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

Related Commands

show 802.11a
show ap stats 802.11a

config 802.11 fragmentation

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

config 802.11{a | b} fragmentation threshold



Note This command can only be used when the network is disabled using the [config 802.11 disable](#) command.

Syntax Description

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

Defaults

None.

Examples

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

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

Related Commands

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

config 802.11 l2roam rf-params

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

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

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

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, we recommend that you set the *trans_time* to 1 second.

Examples

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

```
> config 802.11a l2roam rf-params custom -80 2 -70 7
```

Related Commands

[show advanced 802.11 l2roam](#)
[show l2tp](#)

config 802.11 rate

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

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

Syntax Description

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

Defaults

None.

Usage Guidelines

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

Examples

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

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

Related Commands

show ap config 802.11a
config 802.11b rate

config 802.11 tsm

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

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

Syntax Description

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

Defaults

Disabled.

Examples

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

```
> config 802.11a tsm enable
```

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

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

Related Commands

[show ap stats](#)

[show client tsm](#)

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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures the 802.11 transmit power level for all lightweight access points.
auto	(Optional) Specifies the power level is automatically set by Radio Resource Management (RRM) for the 802.11 Cisco radio.
once	(Optional) Specifies the power level is automatically set once by RRM.
<i>power_level</i>	(Optional) Manual Transmit power level number for the access point.
ap	Configures the 802.11 transmit power level for a specified lightweight access point.
<i>ap_name</i>	Access point name.

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. See 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

This example shows how to automatically set the 802.11a radio transmit power level in all lightweight access points:

```
> config 802.11a txPower global auto
```

This example shows how to manually set the 802.11b radio transmit power to level 5 for all lightweight access points:

```
> config 802.11b txPower global 5
```

This example shows how to automatically set the 802.11b radio transmit power for access point AP1:

```
> config 802.11b txPower AP1 global
```

This example shows how to manually set the 802.11a radio transmit power to power level 2 for access point AP1:

```
> 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]
```

Syntax Description

mgmt	Configures the AAA authentication search order for controller management users by specifying up to three AAA authentication server types. The order that the server types are entered specifies the AAA authentication search order.
<i>aaa_server_type</i>	(Optional) AAA authentication server type (local , radius , or tacacs). The local setting specifies the local database, the radius setting specifies the RADIUS server, and the tacacs setting specifies the TACACS+ server.

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

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

```
> 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

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

Defaults

None.

Examples

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

```
> config aaa auth mgmt radius
```

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

```
> config aaa auth mgmt tacacs
```

Related Commands

show aaa auth order

config acl apply

To apply an access control list (ACL) to the data path, use the **config acl apply** command.

config acl apply *rule_name*

Syntax Description	<i>rule_name</i> ACL name that contains up to 32 alphanumeric characters.
Defaults	None.
Usage Guidelines	For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.
Examples	This example shows how to apply an ACL to the data path: > config acl apply acl01
Related Commands	show acl

config acl counter

To see if packets are hitting any of the access control lists (ACLs) configured on your controller, use the **config acl counter** command.

config acl counter {start | stop}

Syntax Description

start	Enables ACL counters on your controller.
stop	Disables ACL counters on your controller.

Defaults

config acl counter stop

Usage Guidelines

ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

Examples

This example shows how to enable ACL counters on your controller:

```
> config acl counter start
```

Related Commands

clear acl counters
show acl detailed

config acl create

To create a new access control list (ACL), use the **config acl create** command.

config acl create *rule_name*

Syntax Description	<i>rule_name</i> ACL name that contains up to 32 alphanumeric characters.
Defaults	None.
Usage Guidelines	For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.
Examples	This example shows how to create a new ACL: > config acl create ac101
Related Commands	show acl

config acl cpu

To create a new access control list (ACL) rule that restricts the traffic reaching the CPU, use the **config acl cpu** command.

```
config acl cpu rule_name {wired | wireless | both}
```

Syntax Description

wired	Specifies an ACL on wired traffic.
wireless	Specifies an ACL on wireless traffic
both	Specifies an ACL on both wired and wireless traffic.

Defaults

None.

Usage Guidelines

This command allows you to control the type of packets reaching the CPU.

Examples

This 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 access control list (ACL), use the **config acl delete** command.

config acl delete *rule_name*

Syntax Description	<i>rule_name</i> ACL name that contains up to 32 alphanumeric characters.
Defaults	None.
Usage Guidelines	For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.
Examples	This example shows how to delete an ACL named acl101 on the CPU: > config acl delete acl101
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}
```

Syntax Description

action	Configures whether to permit or deny access.
<i>rule_name</i>	ACL name that contains up to 32 alphanumeric characters.
<i>rule_index</i>	Rule index between 1 and 32.
permit	Permits the rule action.
deny	Denies the rule action.
add	Adds a new rule.
change	Changes a rule's index.
index	Specifies a rule index.
delete	Deletes a rule.
destination address	Configures a rule's destination IP address and netmask.
<i>ip_address</i>	IP address of the rule.
<i>netmask</i>	Netmask of the rule.
<i>start_port</i>	Start port number (between 0 and 65535).
<i>end_port</i>	End port number (between 0 and 65535).
direction	Configures a rule's direction to in, out, or any.
in	Configures a rule's direction to in.
out	Configures a rule's direction to out.
any	Configures a rule's direction to any.
dscp	Configures a rule's DSCP.
<i>dscp</i>	Number between 0 and 63, or any .
protocol	Configures a rule's DSCP.
<i>protocol</i>	Number between 0 and 255, or any .
source address	Configures a rule's source IP address and netmask.
source port range	Configures a rule's source port range.
swap	Swap's two rules' indices.

Defaults

None.

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

Examples

This example shows how to configure an ACL to permit access:

```
> 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 7920VSIENConfig

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

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

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

Defaults	None.

Examples	This example shows how to configure the call admission limit for 7920 VISE parameters: <pre>> config advanced 802.11b 7920VSIENConfig call-admission-limit 4</pre>

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 add

To add channel to the 802.11 networks auto RF channel list, use the **config advanced 802.11 channel add** command.

config advanced 802.11{a | b} channel {add | delete} *channel_number*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
add	Adds a channel to the 802.11 network auto RF channel list.
delete	Deletes a channel from the 802.11 network auto RF channel list.
<i>channel_number</i>	Channel number to add to the 802.11 network auto RF channel list.

Defaults

None.

Examples

This example shows how to add a channel to the 802.11a network auto RF channel list:

```
> config advanced 802.11a channel add 132
```

This example shows how to delete a channel from the 802.11a network auto RF channel list:

```
> config advanced 802.11a channel delete 136
```

Related Commands

show advanced 802.11a channel
config advanced 802.11b channel update

config advanced 802.11 channel cleanair-event

To configure cleanair event driven Radio Resource Management (RRM) parameters for all 802.11 Cisco lightweight access points, use the **config advanced 802.11 channel cleanair-event** command.

config advanced 802.11{a | b} channel cleanair-event {enable | disable | sensitivity [low | medium | high]}

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables the cleanair event-driven RRM parameters.
	disable	Disables the cleanair event-driven RRM parameters.
	sensitivity	Sets the sensitivity for cleanair event-driven RRM.
	low	(Optional) Specifies low sensitivity.
	medium	(Optional) Specifies medium sensitivity
	high	(Optional) Specifies high sensitivity

Defaults	None.

Examples	This example shows how to enable the cleanair event-driven RRM parameters:

```
> config advanced 802.11a channel cleanair-event enable
```

This example shows how to set the high sensitivity for cleanair event-driven RRM:

```
> config advanced 802.11a channel cleanair-event sensitivity high
```

Related Commands	show advanced 802.11a channel config advanced 802.11b channel update

config advanced 802.11 channel cleanair-event

To configure cleanair event driven Radio Resource Management (RRM) parameters for all 802.11 Cisco lightweight access points, use the **config advanced 802.11 channel cleanair-event** command.

config advanced 802.11 {a | b} channel cleanair-event {enable | disable | sensitivity [low | medium | high]}

Syntax Description		
a		Specifies the 802.11a network.
b		Specifies the 802.11b/g network.
enable		Enables the cleanair event-driven RRM parameters.
disable		Disables the cleanair event-driven RRM parameters.
sensitivity		Sets the sensitivity for cleanair event-driven RRM.
low		(Optional) Specifies low sensitivity.
medium		(Optional) Specifies medium sensitivity
high		(Optional) Specifies high sensitivity

Defaults	None.

Examples	This example shows how to enable the cleanair event-driven RRM parameters: <pre>> config advanced 802.11a channel cleanair-event enable</pre> This example shows how to set the high sensitivity for cleanair event-driven RRM: <pre>> config advanced 802.11a channel cleanair-event sensitivity high</pre>

Related Commands	show advanced 802.11a channel

config advanced 802.11 channel dca anchor-time

To specify the time of day when the Dynamic Channel Assignment (DCA) algorithm is to start, use the **config advanced 802.11 channel dca anchor-time** command.

config advanced 802.11{a | b} channel dca anchor-time *value*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
<i>value</i>	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

This example shows how to configure the time of delay when the dynamic channel assignment algorithm starts:

```
> 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 Dynamic Channel Assignment (DCA) channel width for all 802.11n radios in the 5-GHz band, use the following command:

```
config advanced 802.11 {a | b} channel dca chan-width-11n {20 | 40}
```

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
20	Sets the channel width for 802.11n radios to 20 MHz.
40	Sets the channel width for 802.11n radios to 40 MHz.

Defaults

The 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 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

This example shows how to add a channel to the 802.11a network auto channel list:

```
> 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 Dynamic Channel Assignment (DCA) is allowed to run, use the **config advanced 802.11 channel dca interval** command.

config advanced 802.11{a | b} channel dca interval *value*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
<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, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.

Examples

This example shows how often the DCA algorithm is allowed to run:

```
> config advanced 802.11a 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 Dynamic Channel Assignment (DCA) algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels, use the **config advanced 802.11 channel dca sensitivity** command.

config advanced 802.11 {a | b} channel dca sensitivity {low | medium | high}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
low	Specifies the DCA algorithm is not particularly sensitive to environmental changes. See the “Usage Guidelines” section for more information.
medium	Specifies the DCA algorithm is moderately sensitive to environmental changes. See the “Usage Guidelines” section for more information.
high	Specifies the DCA algorithm is highly sensitive to environmental changes. See the “Usage Guidelines” section for more information.

Defaults

None.

Usage Guidelines

The DCA sensitivity thresholds vary by radio band as shown in [Table 2-3](#).

To aid in troubleshooting, the output of this command shows an error code for any failed calls. [Table 2-1](#) explains the possible error codes for failed calls.

Table 2-3 DCA Sensitivity Thresholds

Sensitivity	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

Examples

This example shows how to configure the value of DCA algorithm’s sensitivity to low:

```
> 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 Radio Resource Management (RRM) consider or ignore foreign 802.11a interference avoidance in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel foreign** command.

config advanced 802.11{a | b} channel foreign {enable | disable}

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables the foreign access point 802.11a interference avoidance in the channel assignment.
	disable	Disables the foreign access point 802.11a interference avoidance in the channel assignment.

Defaults	Enabled.

Examples	This example shows how 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 Radio Resource Management (RRM) consider or ignore the traffic load in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel load** command.

config advanced 802.11 {a | b} channel load {enable | disable}

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables the Cisco lightweight access point 802.11a load avoidance in the channel assignment.
	disable	Disables the Cisco lightweight access point 802.11a load avoidance in the channel assignment.

Defaults	Disabled.

Examples	This example shows how to have RRM consider the traffic load when making channel selection updates for all 802.11a Cisco lightweight access points: <pre>> config advanced 802.11a channel load enable</pre>

Related Commands	show advanced 802.11a channel config advanced 802.11b channel load

config advanced 802.11 channel noise

To have Radio Resource Management (RRM) consider or ignore non-802.11a noise in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel noise** command.

config advanced 802.11{a | b} channel noise {enable | disable}

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables non-802.11a noise avoidance in the channel assignment. or ignore.
	disable	Disables the non-802.11a noise avoidance in the channel assignment.

Defaults	Disabled.

Examples	This example shows how 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 outdoor-ap-dca

To enable or disable the controller to avoid checking the non-DFS channels, use the **config advanced 802.11 channel outdoor-ap-dca** command.

config advanced 802.11{a | b} channel outdoor-ap-dca {enable | disable}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables 802.11 network dca list option for outdoor access point.
disable	Disables 802.11 network dca list option for outdoor access point.

Defaults

Disabled.

Usage Guidelines

The **config advanced 802.11{a | b} channel outdoor-ap-dca {enable | disable}** command is applicable only for deployments having outdoor access points such as 1522 and 1524.

Examples

This example shows how to enable the 802.11a dca list option for outdoor access point:

```
> config advanced 802.11a channel outdoor-ap-dca enable
```

Related Commands

show advanced 802.11a channel
config advanced 802.11b channel noise

config advanced 802.11 channel update

To have Radio Resource Management (RRM) initiate a channel selection update for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel update** command.

config advanced 802.11{a | b} channel update

Syntax Description

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

Defaults

None.

Examples

This example shows how to initiate a channel selection update for all 802.11a network access points:

```
> 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the coverage hole detection.
disable	Disables the coverage hole detection.

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

This example shows how to enable coverage hole detection on 802.11a network:

```
> 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

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

This example shows how to specify the percentage of clients for all 802.11a access points that are experiencing a low signal level:

```
> 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
data	Specifies the threshold for data packets.
voice	Specifies the threshold for voice packets.
<i>percent</i>	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

This example shows how to configure the threshold count for minimum uplink failures for data packets:

```
> 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 received signal strength indication (RSSI) value at or below the data or voice RSSI threshold, use the **config advanced 802.11 coverage level global** command.

config advanced 802.11{a | b} **coverage level global** *clients*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	<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 This example shows how to specify the minimum number of clients on all 802.11a access points with an RSSI value at or below the RSSI threshold:

```
> 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
data	Specifies the threshold for data packets.
voice	Specifies the threshold for voice packets.
<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

This example shows how to configure the failure count threshold for uplink data packets:

```
> 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
data	Specifies the threshold for data packets.
voice	Specifies the threshold for voice packets.
<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, 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

This example shows how to configure the minimum receive signal strength indication threshold value for data packets that are received by an 802.11a access point:

```
> 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 | custom-voice}

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

Defaults wmm-default

Examples This example shows how to enable Spectralink voice priority parameters:

```
> 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

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

Defaults

None.

Examples

This example shows how to return all the 802.11a advanced settings to their factory defaults:

```
> config advanced 802.11a factory
```

Related Commands

show advanced 802.11a channel

config advanced 802.11 group-member

To configure members in 802.11 static RF group, use the **config advanced 802.11 group-member** command.

config advanced 802.11{a | b} group-member {add | remove} controller controller-ip-address

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
add	Adds a controller to the static RF group.
remove	Removes a controller from the static RF group.
<i>controller</i>	Name of the controller to be added.
<i>controller-ip-address</i>	IP address of the controller to be added.

Defaults

None.

Examples

This example shows how to add a controller in the the 802.11a automatic RF group:

```
> config advanced 802.11a group-member add cisco-controller 209.165.200.225
```

Related Commands

show advanced 802.11a group
config advanced 802.11 group-mode

config advanced 802.11 group-mode

To set the 802.11a automatic RF group selection mode on or off, use the **config advanced 802.11 group-mode** command.

config advanced 802.11 {a | b} group-mode {auto | leader | off | restart}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
auto	Sets the 802.11a RF group selection to automatic update mode.
leader	Sets the 802.11a RF group selection to static mode, and sets this controller as the group leader.
off	Sets the 802.11a RF group selection to off.
restart	Restarts the 802.11a RF group selection.

Defaults

Auto.

Examples

This example shows how to turn the 802.11a automatic RF group selection mode on:

```
> config advanced 802.11a group-mode auto
```

This example shows how 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 802.11 group-member

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	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	logging channel	Logs channel changes.
	on	Enables the 802.11 channel logging.
	off	Disables 802.11 channel logging.

Defaults Off (disabled).

Examples This example shows how to turn the 802.11a logging channel selection mode on:
> **config advanced 802.11a 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 coverage profile violation logging.
off	Disables the 802.11 coverage profile violation logging.

Defaults

Off (disabled).

Examples

This example shows how to turn the 802.11a coverage profile violation logging selection mode on:

```
> 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 foreign interference profile violation logging.
off	Disables the 802.11 foreign interference profile violation logging.

Defaults

Off (disabled).

Examples

This example shows how to turn the 802.11a foreign interference profile violation logging selection mode on:

```
> 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 load profile violation logging.
off	Disables the 802.11 load profile violation logging.

Defaults

Off (disabled).

Examples

This example shows how to turn the 802.11a load profile logging mode on:

```
> 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 noise profile violation logging.
off	Disables the 802.11 noise profile violation logging.

Defaults

Off (disabled).

Examples

This example shows how to turn the 802.11a noise profile logging mode on:

```
> 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 performance profile violation logging.
off	Disables the 802.11 performance profile violation logging.

Defaults

Off (disabled).

Examples

This example shows how to turn the 802.11a performance profile logging mode on:

```
> config advanced 802.11a 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 transmit power change logging.
off	Disables the 802.11 transmit power change logging.

Defaults

Off (disabled).

Examples

This example shows how to turn the 802.11a transmit power change mode on:

```
> config advanced 802.11a 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
all	Monitors all channels.
country	Monitors the channels used in the configured country code.
dca	Monitors the channels used by the automatic channel assignment.

Defaults

country.

Examples

This example shows how to monitor the channels used in the configured country:

```
> 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
<i>seconds</i>	Coverage measurement interval between 60 and 3600 seconds.

Defaults

180 seconds.

Examples

This example shows how to set the coverage measurement interval to 60 seconds:

```
> config advanced 802.11a 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
<i>seconds</i>	Load measurement interval between 60 and 3600 seconds.

Defaults

60 seconds.

Examples

This example shows how 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the 802.11 access point monitoring.
disable	Disables the 802.11 access point monitoring.

Defaults

Enabled.

Examples

This example shows how to enable the 802.11a access point monitoring:

```
> 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 ndp-type

To configure 802.11 access point radio resource management neighbor discovery protocol type, use the **following** command:

```
config advanced 802.11 {a | b} monitor ndp-type {protected | transparent}
```

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
protected	Specifies the Tx RRM protected neighbor discovery protocol.
transparent	Specifies the Tx RRM transparent neighbor discovery protocol.

Defaults

None.

Usage Guidelines

Before you configure the 802.11 access point RRM neighbor discovery protocol type, ensure that you have disabled the network by entering the **config 802.11 disable network** command.

Examples

This example shows how to enable the 802.11a access point RRM neighbor discovery protocol type as protected:

```
> config advanced 802.11a monitor ndp-type protected
```

Related Commands

[show advanced 802.11 monitor](#)
[config advanced 802.11 monitor mode](#)
[config 802.11 disable](#)

config advanced 802.11 monitor noise

To set the 802.11a noise measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor noise** command.

config advanced 802.11{a | b} monitor noise *seconds*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
<i>seconds</i>	Noise measurement interval between 60 and 3600 seconds.

Defaults

180 seconds.

Examples

This example shows how 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
<i>seconds</i>	Signal measurement interval between 60 and 3600 seconds.

Defaults

60 seconds.

Examples

This example shows how 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access points.
<i>cisco_ap</i>	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

This example shows how 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.

This example shows how 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
<i>cisco_ap</i>	Cisco lightweight access point.
on	Customizes performance profiles for this Cisco lightweight access point.
off	Uses global default performance profiles for this Cisco lightweight access point.

Defaults

Off.

Examples

This example shows how 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access points.
<i>cisco_ap</i>	Cisco lightweight access point name.
<i>percent</i>	802.11a foreign 802.11a interference threshold between 0 and 100 percent.

Defaults

10.

Examples

This example shows how to set the foreign 802.11a transmitter interference threshold for all Cisco lightweight access points to 50 percent:

```
> config advanced 802.11a profile foreign global 50
```

This example shows how to set the foreign 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access point specific profiles.
<i>cisco_ap</i>	Cisco lightweight access point name.
<i>dBm</i>	802.11a foreign noise threshold between –127 and 0 dBm.

Defaults

–70 dBm.

Examples

This example shows how 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
```

This example shows how 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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access point specific profiles.
<i>cisco_ap</i>	Cisco lightweight access point name.
<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

This example shows how to set all Cisco lightweight access point data-rate thresholds to 1000 bytes per second:

```
> config advanced 802.11a profile throughput global 1000
```

This example shows how to set the AP1 data-rate threshold to 10000000 bytes per second:

```
> config advanced 802.11a profile throughput 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. The operating system generates a trap when this threshold is exceeded.

config advanced 802.11{a | b} **profile utilization** {global | cisco_ap} percent

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures a global Cisco lightweight access point specific profile.
<i>cisco_ap</i>	Specifies Cisco lightweight access point name.
<i>percent</i>	802.11a RF utilization threshold between 0 and 100 percent.

Defaults

80 percent.

Examples

This example shows how to set the RF utilization threshold for all Cisco lightweight access points to 0 percent:

```
> config advanced 802.11a profile utilization global 0
```

This example shows how 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
```

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	receiver	Specifies the receiver configuration
	default	Specifies the default advanced receiver configuration.
	rxstartjumpThreshold	Specifies the receiver start signal.
	<i>value</i>	Jump threshold configuration value between 0 and 127.

Defaults	None.

Examples	This example shows how to prevent changes to receiver parameters while the network is enabled: <pre>> config advanced802.11a receiver default</pre>

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

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

Defaults

None.

Examples

This example shows how to initiate updates of 802.11a transmit power for an 802.11a access point:

```
> 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	<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	This example shows how to configure the primary backup controller: > 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 secondary 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

<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

This example shows how to configure a secondary backup controller:

```
> 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	<i>num_of_retries</i> Number of excessive retries before client handoff (from 0 to 255).
Defaults	0 excessive retries (disabled).
Usage Guidelines	This command is supported only for the 1000/1510 series access points.
Examples	This example shows how 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

enable	Enables this command.
disable	Disables this command.

Defaults

Disabled.

Examples

This example shows how to enable over-the-air frame padding:

```
> 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** [*number of associations per interval* | *interval in milliseconds*] | **disable**}

Syntax Description	enable	Enable this feature.
	disable	Disables this feature.
	<i>number of associations per interval</i>	(Optional) Number of association request per access point slot in a given interval. The valid range is 1 to 100.
	<i>interval in milliseconds</i>	(Optional) 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 This example shows how to configure the number of association requests per access point slot in a given interval of 20 with the association request limit interval of 250:

```
> 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 <i>timeout</i>	(Optional) Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK.	The default value is 1000 milliseconds.
eapol-key-retries <i>retries</i>	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client.	The default value is 2.
identity-request-timeout <i>timeout</i>	(Optional) Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client.	The default value is 30 seconds.
identity-request-retries	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client.	The default value is 2.
key-index <i>index</i>	(Optional) <i>index</i> —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.	
enable	Ignores the same username reaching the maximum EAP identity response.	
disable	Checks the same username reaching the maximum EAP identity response.	
request-timeout	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client.	The default value is 30 seconds.
request-retries	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client.	The default value is 2.

Defaults

Default for **eapol-key-timeout**: 1 second.

Default for **eapol-key-retries**: 2 retries.

Examples

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

```
> 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

enable	Enables the switch control path rate limiting feature.
disable	Disables the switch control path rate limiting feature.

Defaults

None.

Examples

This example shows how to enable switch control path rate limiting:

```
> config advanced rate enable
```

config advanced sip-preferred-call-no

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

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

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

Defaults None.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

[config wlan qos](#)
[config 802.11 cac video acm](#)
[config 802.11 cac voice acm](#)
[config wlan call-snoop](#)
[show ap stats](#)

config advanced 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	enable	Enables the switch port statistics collection.
	disable	Disables the switch port statistics collection.

Defaults Enabled.

Examples This example shows how to disable the switch port statistics collection settings:
> 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

enable	Enables the filtering of probe requests.
disable	Disables the filtering of probe requests.

Defaults

None.

Examples

This example shows how to enable the filtering of probe requests forwarded from an access point to the controller:

```
> config advanced probe filter enable
```

Related Commands

[config advanced probe limit](#)
[config radius acct ipsec authentication](#)
[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	<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 The default *num_probes* is 2 probe requests.
The default *interval* is 500 milliseconds.

Examples This example shows how to set the number of probes per access point per client to 5 and the probe interval to 800 milliseconds:

```
> config advanced probe limit 5 800
```

Related Commands [config advanced probe filter](#)
[config radius acct ipsec authentication](#)
[show advanced probe](#)

Configure Advanced Timers Commands

User the **advanced timers** commands to configure advanced 802.11a settings.

config advanced timers ap-discovery-timeout

To configure the Cisco lightweight access point discovery time-out, use the **config advanced timers ap-discovery-timeout** command.

config advanced timers ap-discovery-timeout *seconds*

Syntax Description	<i>seconds</i> Cisco lightweight access point discovery timeout value between 1 and 10 seconds.
Defaults	10 seconds.
Usage Guidelines	The Cisco lightweight access point discovery timeout is how often a Cisco wireless LAN controller attempts to discover unconnected Cisco lightweight access points.
Examples	This example shows how to configure an access point discovery-timeout with the timeout value of 20: <pre>> config advanced timers ap-discovery-timeout 20</pre>
Related Commands	show advanced timers config advanced timers ap-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 which reduces 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		
local		Configures the fast heartbeat interval for access points in local mode only.
hreap		Configures the fast heartbeat interval for access points in hybrid-REAP mode only.
all		Configures the fast heartbeat interval for all access points.
enable		Enables the fast heartbeat interval.
disable		Disables the fast heartbeat interval.
<i>interval</i>		Small heartbeat interval (between 1 and 10 seconds, inclusive), which reduces the amount of time it takes to detect a controller failure.

Defaults

Disabled.

Examples

This example shows how to enable the fast heartbeat interval for access point in local mode:

```
> config advanced timers ap-fast-heartbeat local enable 5
```

This example shows how to enable the fast heartbeat interval for access point in hybrid-REAP mode:

```
> config advanced timers ap-fast-heartbeat hreap enable 8
```

This example shows how to enable the fast heartbeat interval for all access points:

```
> config advanced timers ap-fast-heartbeat all enable 6
```

This example shows how to disable the fast heartbeat interval for all access point:

```
> 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

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

seconds Cisco lightweight access point heartbeat timeout value between 1 and 30 seconds.

Defaults

30 seconds.

Usage Guidelines

The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keep-alive signal to the Cisco wireless LAN controller.

This *seconds* value should be at least three times larger than the fast heartbeat timer.

Examples

This example shows how to configure an access point heartbeat timeout to 20:

```
> config advanced timers ap-heartbeat-timeout 20
```

Related Commands

[show advanced timers](#)
[config advanced timers ap-discovery-timeout](#)
[config advanced timers ap-fast-heartbeat](#)
[config advanced timers ap-primary-discovery-timeout](#)
[config advanced timers auth-timeout](#)

config advanced timers ap-primary-discovery-timeout

To configure the access point primary discovery request timer, use the **config advanced timers ap-primary-discovery-timeout** command.

config advanced timers ap-primary-discovery-timeout *interval*

Syntax Description	<i>interval</i> Access point primary discovery request timer between 30 and 3600 seconds.
Defaults	120 seconds.
Examples	This example shows how to configure the access point primary discovery request timer to 1200 seconds: <pre>> config advanced timers ap-primary-discovery-timeout 1200</pre>
Related Commands	show advanced timers config advanced timers ap-discovery-timeout config advanced timers ap-fast-heartbeat config advanced timers ap-heartbeat-timeout config advanced timers auth-timeout

config advanced timers auth-timeout

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

config advanced timers auth-timeout *seconds*

Syntax Description	<i>seconds</i>	Authentication response timeout value in seconds between 10 and 600.

Defaults	10 seconds.

Examples	This example shows how to configure the authentication timeout to 20 seconds: <pre>> config advanced timers auth-timeout 20</pre>

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

config advanced timers eap-timeout *seconds*

Syntax Description	<i>seconds</i> EAP timeout value in seconds between 8 and 120.
Defaults	None.
Examples	This example shows how to configure the EAP expiration timeout to 10 seconds: > config advanced timers eap-timeout 10
Related Commands	show advanced timers

config advanced timers eap-identity-request-delay

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

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

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

Defaults	None.

Examples	This example shows how to configure the advanced EAP identity request delay to 8 seconds: > config 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

Use 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** command.

config ap [{enable | disable} *cisco_ap* | {add | delete} *MAC* *port* {enable | disable} *IP_address*]

Syntax Description

enable	Enables the Cisco lightweight access point.
disable	Disables the Cisco lightweight access point.
<i>cisco_ap</i>	Name of the Cisco lightweight access point.
add	Adds foreign access points.
delete	Deletes foreign access points.
<i>MAC</i>	MAC address of a foreign access point.
<i>port</i>	Port number through which the foreign access point can be reached.
<i>IP_address</i>	IP address of the foreign access point.

Defaults

None.

Examples

This example shows how to disable lightweight access point AP1:

```
> config ap disable AP1
```

This example shows how to add a foreign access point with MAC address 12:12:12:12:12:12 and IP address 192.12.12.1 from port 2033:

```
> 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 bhrate

To configure the Cisco bridge backhaul Tx rate, use the **config ap bhrate** command.

config ap bhrate {*rate* | **auto**} *cisco_ap*

Syntax Description	<i>rate</i>	Cisco bridge backhaul Tx rate in kbps. The valid values are 6000, 12000, 18000, 24000, 36000, 48000, and 54000.
	auto	Configures the auto data rate.
	<i>cisco_ap</i>	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	This example shows how to configure the Cisco bridge backhaul Tx rate to 54000 kbps: <pre>> config ap bhrate 54000 AP01</pre>

Related Commands	config ap

config ap autoconvert

When access points in local mode connect to a Cisco 7500 Series Controller, they do not serve clients. The access point details are available in the controller. To enable access points to serve clients or perform monitoring related tasks when connected to the Cisco 7500 Series Controller, the access points must be in hybrid-REAP mode or monitor mode. To automatically convert all access points to a hybrid-REAP mode or monitor mode upon joining the controller, use the **config ap autoconvert** command:

config ap autoconvert {hheap | monitor | disable}

Syntax Description	hheap	Configures all the APs automatically to H-REAP mode.
	monitor	Configures all the APs automatically to monitor mode.
	disable	Disables the autoconvert option on the APs.

Defaults	None.

Examples	This example shows how to automatically convert all APs to the H-REAP mode:

```
> config ap autoconvert hheap
```

This example shows how to disable the autoconvert option on the APs:

```
> config ap autoconvert disable
```

Related Commands	Configure Access Point Commands Show Access Point Commands

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

<i>rate</i>	Cisco bridge backhaul Tx rate in kbps. The valid values are 6000, 12000, 18000, 24000, 36000, 48000, and 54000.
auto	Configures the auto data rate.
<i>cisco_ap</i>	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

This example shows how to configure the Cisco bridge backhaul Tx rate to 54000 kbps:

```
> 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

set	Sets a Cisco lightweight access point's bridge group name.
<i>groupname</i>	<i>Bridge group name.</i>
delete	Deletes 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

This example shows how to delete a bridge group name on Cisco access point's bridge group name AP02:

```
> 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	enable	Enables the Ethernet-to-Ethernet bridging on a Cisco lightweight access point.
	disable	Disables Ethernet-to-Ethernet bridging.
	<i>cisco_ap</i>	Name of a Cisco lightweight access point.

Defaults None.

Examples This example shows how to enable bridging on an access point:

```
> config ap bridging enable nyc04-44-1240
```

This example shows how to disable bridging on an access point:

```
> config ap bridging disable nyc04-44-1240
```

Related Commands **config ap**

config ap cdp

To enable or disable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **config ap cdp** command.

```
config ap cdp {enable | disable | interface {ethernet interface_number | slot slot_id}} {cisco_ap | all}
```

Syntax Description

enable	Enables CDP on an access point.
disable	Disables CDP on an access point.
interface	Configures CDP in a specific interface.
ethernet	Configures CDP for an ethernet interface.
<i>interface_number</i>	Ethernet interface number between 0 and 3.
slot	Configures CDP for a radio interface.
<i>slot_id</i>	Slot number between 0 and 3.
<i>cisco_ap</i>	Name of a Cisco lightweight access point.
all	Specifies all access points.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

Enabled on radio interfaces of mesh APs and disabled on radio interfaces of non-mesh APs. Enabled on Ethernet interfaces of all APs.

Usage Guidelines

The **config ap cdp disable all** command disables CDP on all access points that are joined to the controller and all access points that join in the future. CDP remains disabled on both current and future access points even after the controller or access point reboots. To enable CDP, enter the **config ap cdp enable all** command.



Note

CDP over Ethernet/radio interfaces is available only when CDP is enabled. After you enable CDP on all access points joined to the controller, you may disable and then reenabling CDP on individual access points using the **config ap cdp {enable | disable} cisco_ap** command. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.

Examples

This example shows how to enable CDP on all access points:

```
> config ap cdp enable all
```

This example shows how to disable CDP on ap02 access point:

```
> config ap cdp disable ap02
```

This example shows how to enable CDP for Ethernet interface number 2 on all access points:

```
> config ap cdp interface ethernet 2 enable all
```

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

enable	Enables the Cisco lightweight access point's memory core dump setting.
disable	Disables the Cisco lightweight access point's memory core dump setting.
<i>tftp_server_ipaddress</i>	IP address of the TFTP server to which the access point sends core dump files.
<i>filename</i>	Name the access point uses to label the core file.
compress	Compresses the core dump file.
uncompress	Uncompresses the core dump file.
<i>cisco_ap</i>	Name of a Cisco lightweight access point.
all	Specifies all access points.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

None.

Usage Guidelines

The access point must be able to reach the TFTP server.

Examples

This example shows how to configure and compress the core dump file:

```
> 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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to delete all crash files: <pre>> config ap crash-file clear-all</pre>

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	<i>filename</i>	Name of the file to delete.

Defaults	None.

Examples	This example shows how to delete crash file 1: > 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.

config ap crash-file get-crash-file *cisco_ap*

Syntax Description	<i>cisco_ap</i> Name of the Cisco lightweight access point.
Defaults	None.
Usage Guidelines	Use the transfer upload datatype command to transfer the collected data to the Cisco wireless LAN controller.
Examples	This example shows how to collect the latest crash data for access point AP3: > 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	slot_id	Slot ID (either 0 or 1).
	cisco_ap	Name of a Cisco lightweight access point.

Defaults	None.

Examples	This example shows how to collect the radio core dump for access point AP02 and slot 0: <pre>> config ap crash-file get-radio-core-dump 0 AP02</pre>

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, use the `config ap dot1xuser` command.

```
config ap dot1xuser add username user password password {all | cisco_ap}
```

Syntax Description	add username	Specifies to add a username.
	<i>user</i>	Username.
	password	Specifies to add a password.
	<i>password</i>	Password.
	<i>cisco_ap</i>	Specific access point.
	all	Specifies all access points.

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 uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

You can set the values for a specific access point.

Examples This example shows how to configure the global authentication username and password for all access points:

```
> config ap dot1xuser add username cisco123 password cisco2020 all
```

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, use the **config ap dot1xuser delete** command.

config ap dot1xuser delete *cisco_ap*

Syntax Description

<i>cisco_ap</i>	Access point.

Defaults

None.

Examples

This example shows how to delete access point AP01 to use the controller's global authentication settings:

```
> config ap dot1xuser delete AP01
```

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, use the `config ap dot1xuser disable` command.

config ap dot1xuser disable {all | *cisco_ap*}

Syntax Description

disable	Disables authentication.
all	Specifies all access points.
<i>cisco_ap</i>	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

This example shows how to disable the authentication for access point `cisco_ap1`:

```
> config ap dot1xuser disable cisco_ap1
```

Related Commands

[config ap dot1xuser](#)
[config ap dot1xuser delete](#)
[show ap summary](#)

config ap ethernet

To configure the duplex and speed settings on the wireless LAN and the lightweight access points, use the **config ap ethernet** command.

config ap ethernet duplex [auto | half | full] speed [auto | 10 | 100 | 1000] {all | cisco_ap}

Syntax Description

duplex	Specifies the Ethernet port duplex settings.
auto	(Optional) Specifies the Ethernet port duplex auto settings.
half	(Optional) Specifies the Ethernet port duplex half settings.
full	(Optional) Specifies the Ethernet port duplex full settings.
speed	Specifies the Ethernet port speed settings.
auto	(Optional) Specifies the Ethernet port speed to auto.
10	(Optional) Specifies the Ethernet port speed to 10 Mbps.
100	(Optional) Specifies the Ethernet port speed to 100 Mbps.
1000	(Optional) Specifies the Ethernet port speed to 1000 Mbps.
all	Specifies the Ethernet port setting for all connected access points.
<i>cisco_ap</i>	Cisco access point.

Defaults

None

Examples

This example shows how to configure the Ethernet port duplex half settings 10 Mbps for all access points:

```
> config ap ethernet duplex half speed 10 all
```

Related Commands

[config ap](#)
[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.

config ap group-name *groupname* *cisco_ap*

Syntax Description	<i>groupname</i>	Descriptive name for the access point group.
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults	None.

Usage Guidelines	The Cisco lightweight access point must be disabled before changing this parameter.

Examples	This example shows how to configure a descriptive name for access point AP01: <pre>> config ap group-name superusers AP01</pre>

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

primary	Specifies the primary RADIUS server for a specific hybrid-REAP access point.
secondary	Specifies the secondary RADIUS server for a specific hybrid-REAP access point.
<i>ip_address</i>	Name of the Cisco lightweight access point.
<i>auth_port secret</i>	Name of the port.

Defaults

None.

Examples

This example shows how to configure a primary RADIUS server for a specific access point:

```
> 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	enable	Enables the access point's VLAN tagging.
	disable	Disables the access point's VLAN tagging.
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults Disabled. Once enabled, WLANs enabled for local switching inherit the VLAN assigned at the controller.

Examples This example shows how to enable the access point's VLAN tagging for a hybrid-REAP access:

```
> config ap h-reap vlan 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	<i>vlan-id</i>	VLAN identifier.
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults	None.

Examples	This example shows how to configure a native VLAN for a hybrid-REAP access point mode: > 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	<i>ip_address</i>	Name of the Cisco lightweight access point.
	<i>vlan-id</i>	VLAN identifier.
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults	VLAN ID associated to the WLAN.

Examples	This example shows how to assign a VLAN ID to a hybrid-REAP access point:

```
> 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 image predownload

To configure an image on a specified access point, use the **config ap image predownload** command.

config ap image predownload {primary | backup} {cisco_ap | all}

Syntax Description

primary	Predownloads an image to a Cisco access point from the controller's primary image.
backup	Predownloads an image to a Cisco access point from the controller's backup image.
<i>cisco_ap</i>	Name of a Cisco lightweight access point.
all	Specifies all access points to predownload an image.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

None.

Examples

This example shows how to predownload an image to an access point from the primary image:

```
> config ap image predownload primary all
```

Related Commands

config ap image swap
show ap image

config ap image swap

To swap an access point's primary and backup images, use the **config ap image swap** command.

config ap image swap {*cisco_ap* | *all*}

Syntax Description

<i>cisco_ap</i>	Name of a Cisco lightweight access point.
all	Specifies all access points to interchange the boot images.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

None.

Examples

This example shows how to swap an access point's primary and secondary images:

```
> config ap image swap all
```

Related Commands

config ap image predownload
show ap image

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

enable	Enables the access point's LED state.
disable	Disables the access point's LED state.
<i>cisco_ap</i>	Name of a Cisco lightweight access point.
all	Specifies all access points.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

None.

Examples

This example shows how to enable the LED state for an access point:

```
> config ap led-state enable AP02
```

Related Commands

config ap

config ap link-encryption

To enable or disable the 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

enable	Enables the DTLS data encryption for access points.
disable	Disables the DTLS data encryption for access points.
<i>cisco_ap</i>	Name of a Cisco lightweight access point.
all	Specifies all access points.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points.

Usage Guidelines

Only Cisco 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 Cisco 1130, 1140, 1240, and 1250 series access points support DTLS data encryption, and data-encrypted access points can join a Cisco 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

This example shows how to enable the data encryption for an access point:

```
> 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, use the **config ap link-latency** command:

```
config ap link-latency {enable | disable | reset} {cisco_ap | all}
```

Syntax Description

enable	Enables the link latency for an access point.
disable	Disables the link latency for an access point.
reset	Resets all link latency for all access points.
<i>cisco_ap</i>	Name of the Cisco lightweight access point.
all	Specifies all access points.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

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

This example shows how to enable the link latency for all access points:

```
> 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.

config ap location *location cisco_ap*

Syntax Description	<i>location</i>	Location name of the access point (enclosed by double quotation marks).
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults	None.

Usage Guidelines	The Cisco lightweight access point must be disabled before changing this parameter.

Examples	This example shows how to configure the descriptive location for access point AP1: <pre>> config ap location "Building 1" AP1</pre>

Related Commands	show ap summary

config ap logging syslog level

To set the severity level for filtering syslog messages for a particular access point or for all access points, use the **config ap logging syslog level** command.

config ap logging syslog level *severity_level* {*cisco_ap* | **all**}

Syntax Description

severity_level

Severity levels are as follows:

- emergencies—Severity level 0
- alerts—Severity level 1
- critical—Severity level 2
- errors—Severity level 3
- warnings—Severity level 4
- notifications—Severity level 5
- informational—Severity level 6
- debugging—Severity level 7

cisco_ap

Cisco access point.

all

Specifies all access points.



Note

If an AP itself is configured with the name ‘all’, then the ‘all access points’ case takes precedence over the AP that is named ‘all’.

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

This example shows how to set the severity for filtering syslog messages to 3:

```
> config ap logging syslog level 3
```

Related Commands

config logging syslog host
config logging syslog facility
show logging

config ap mgmtuser add

To configure username, password, and secret password for AP management, use the **config ap mgmtuser add** command.

```
config ap mgmtuser add username AP_username password AP_password secret secret  
          {all | cisco_ap}
```

Syntax Description	username	Configures the username for AP management.
	<i>AP_username</i>	Management username.
password	Configures the password for AP management.	
	<i>AP_password</i>	AP management password.
secret	Configures the secret password for privileged AP management.	
	<i>secret</i>	AP management secret password.
all	Applies configuration to every AP that does not have a specific username.	
	<i>cisco_ap</i>	Cisco access point.

Defaults None.

Usage Guidelines

The following requirements are enforced on the password:

- The password should contain characters from at least three of the following classes: lower-case letters, upper-case letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain management username or reverse of username.
- The password should not contain words like Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting \$ for s.

The following requirement is enforced on the secret password:

- The secret password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, or special characters.

Examples

This example shows how to add a username, password, and secret password for AP management:

```
> config ap mgmtuser add username acd password Arc_1234 secret Mid_45 all
```

Related Commands [config ap mgmtuser delete](#)

config ap mgmtuser delete

To force a specific access point to use the controller's global credentials, use the config ap mgmtuser delete command.

config ap mgmtuser delete *cisco_ap*

Syntax Description

<i>cisco_ap</i>	Access point.

Defaults

None.

Examples

This example shows how to delete the credentials of an access point:

```
> config ap mgmtuser delete cisco_ap1
```

Related Commands

[show ap summary](#)

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 | se-connect  
monitor [submode {none | wips}]} cisco_ap
```

Syntax Description	
bridge	Converts from a lightweight access point to a mesh access point (bridge mode).
h-reap	Enables hybrid remote edge access point mode on an access point.
local	Converts from an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point (local mode).
reap	Enables remote edge access point mode on an access point.
rogue	Enables wired rogue detector mode on an access point.
sniffer	Enables wireless sniffer mode on an access point.
se-connect	Enables spectrum expert mode on an access point.
submode	(Optional) Configures wIPS submode on an access point.
none	Disables the wIPS on an access point.
wips	Enables the wIPS submode on an access point.
<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults Local.

Usage Guidelines The sniffer mode captures and forwards all the packets from the clients on that channel to a remote machine that runs AiroPeek or other supported packet analyzer software. It includes information on the timestamp, signal strength, packet size and so on.

Examples This example shows how to set the controller to communicate with access point AP91 in bridge mode:

```
> config ap mode bridge AP91
```

This example shows how to set the controller to communicate with access point AP01 in local mode:

```
> config ap mode local AP01
```

This example shows how to set the controller to communicate with access point AP91 in remote office (REAP) mode:

```
> config ap mode reap AP91
```

This example shows how to set the controller to communicate with access point AP91 in remote office (REAP) mode:

```
> config ap mode h-reap AP01
```

This example shows how to set the controller to communicate with access point AP91 in a wired rogue access point detector mode:

```
> config ap mode rogue AP91
```

This example shows how to set the controller to communicate with access point AP02 in wireless sniffer mode:

```
> config ap mode sniffer AP02
```

This example shows how to set 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	802.11b fast-channel	Configures 802.11b scanning channels for a monitor-mode access point.
	no-optimization	Specifies no channel scanning optimization for the access point.
	tracking-opt	Enables tracking optimized channel scanning for the access point.
	wips-optimized	Enables wIPS optimized channel scanning for the access point.
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults	None.

Examples	This example shows how to configure a Cisco wireless intrusion prevention system (wIPS) monitor mode on access point AP01:

```
> 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

<i>new_name</i>	Desired Cisco lightweight access point name.
<i>old_name</i>	Current Cisco lightweight access point name.

Defaults

None.

Examples

This example shows how to modify the name of access point AP1 to AP2:

```
> 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	<i>MAC</i>	Foreign Access Point MAC address.
	<i>port</i>	Port number for accessing the foreign access point.

Defaults	None.

Examples	This example shows how to configure the port for a foreign access point MAC address: <pre>> config ap port 12:12:12:12:12:12 20</pre>

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

enable	Enables the power injector state for an access point.
disable	Disables the power injector state for an access point.
<i>cisco_ap</i>	Name of the Cisco lightweight access point.
all	Specifies all Cisco lightweight access points connected to the controller.
installed	Detects the MAC address of the current switch port that has a power injector.
override	Overrides the safety checks and assumes a power injector is always installed.
<i>switch_MAC</i>	MAC address of the switch port with an installed power injector.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

None.

Examples

This example shows how to enable the power injector state for all access points:

```
> 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	enable	Enables the inline power Cisco pre-standard switch state for an access point.
	disable	Disables the inline power Cisco pre-standard switch state for an access point.
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults	Disabled.

Examples	This example shows how to enable the inline power Cisco pre-standard switch state for access point AP02:

```
> 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.

```
config ap primary-base controller_name cisco_ap [controller_ip_address]
```

Syntax Description

controller_name	Name of the Cisco wireless LAN controller.
cisco_ap	Cisco lightweight access point name.
controller_ip_address	(Optional) If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller.
Note For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.	

Defaults

None.

Usage Guidelines

The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operations and in the event of a hardware reset.

OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.

Examples

This example shows how to set an access point primary Wireless LAN controller:

```
> 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.

config ap priority {1 | 2 | 3 | 4} cisco_ap

Syntax Description

1	Specifies low priority.
2	Specifies medium priority.
3	Specifies high priority.
4	Specifies the highest (critical) priority.
<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults

1 - Low priority.

Usage Guidelines

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.

Examples

This example shows how to assign a priority designation to access point AP02 that allows it to reauthenticate after a controller failure by assigning a reauthentication priority 3:

```
> 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 reporting-period** command.

config ap reporting-period *period*

Syntax Description

<i>period</i>	Time period in seconds between 10 and 120.

Defaults

None.

Examples

This example shows how to reset an access point reporting period to 120 seconds:

```
> 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	<i>cisco_ap</i> Cisco lightweight access point name.
Defaults	None.
Examples	This example shows how to reset an access point: > config ap reset AP2
Related Commands	show ap config

config ap retransmit interval

To configure the access point control packet retransmission interval, use the **config ap retransmit interval** command.

```
config ap retransmit interval seconds {all | cisco_ap}
```

Syntax Description	seconds	The AP control packet retransmission timeout between 2 and 5 seconds.
	all	All access points.
	cisco_ap	Cisco lightweight access point name.

Defaults None.

Examples This example shows how to configure the retransmission interval for all access points globally:
> config ap retransmit interval 4 all

Related Commands [show ap config](#)

config ap retransmit count

To configure the access point control packet retransmission count, use the **config ap retransmit count** command.

config ap retransmit count *count* {**all** | *cisco_ap*}

Syntax Description

<i>count</i>	Number of times control packet will be retransmitted (range is 3 to 8 times).
all	All access points.
<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults

None.

Examples

This example shows how to configure the retransmission retry count for a specific access point:

```
> config ap retransmit count 6 cisco_ap
```

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} cisco_ap
```

Syntax Description	rootAP	Designates the mesh access point as a root access point (RAP).
	meshAP	Designates the mesh access point as a mesh access point (MAP).
	cisco_ap	Name of the Cisco lightweight access point.

Defaults meshAP.

Usage Guidelines Use the **meshAP** keyword if the access point has a wireless connection to the controller, or use the **rootAP** keyword if the access point has a wired connection to the controller.

Examples This example shows how to designate mesh access point AP02 as a root access point:

```
> 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	enable	Enables the Reset button for an access point.
	disable	Disables the Reset button for an access point.
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.

Defaults	None.

Examples	This example shows how to configure the reset button for access point AP03: <pre>> config ap rst-button enable AP03</pre>

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.

config ap secondary-base *controller_name* *cisco_ap* [*controller_ip_address*]

Syntax Description

<i>controller_name</i>	Name of the 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

The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operations and in the event of a hardware reset.

OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.

Examples

This example shows how to set an access point secondary Cisco wireless controller:

```
> 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	802.11a	Specifies the 802.11a network.
	802.11b	Specifies the 802.11b network.
	enable	Enables sniffing on an access point.
	<i>channel</i>	Channel to be sniffed.
	<i>server_ip</i>	IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark software.
	disable	Disables sniffing on an access point.
	<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 Omnipeek, Airopeek, AirMagnet, or Wireshark software. It includes information on the timestamp, signal strength, packet size and so on.

Before an access point can act as a sniffer, a remote computer that runs one of the listed packet analyzers must be set up so that it can receive packets sent by the access point. After the Airopeek installation, copy the following .dll files to the location where airopeek is installed:

- **socket.dll** file to the **Plug-ins** folder (for example, *C:\Program Files\WildPackets\AiroPeek\Plugins*)
- **socketres.dll** file to the **PluginRes** folder (for example, *C:\Program Files\WildPackets\AiroPeek\1033\PluginRes*)

Examples This example shows how to enable the sniffing on the 802.11a an access point primary Wireless LAN controller:

```
> 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.

```
config ap ssh {enable | disable} cisco_ap
```

Syntax Description	enable	Enables the SSH connectivity on an access point.
	disable	Disables the SSH connectivity on an access point.
	<i>cisco_ap</i>	Cisco access point name.

Defaults None.

Usage Guidelines The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operation and in the event of a hardware reset.

Examples This example shows how to enable SSH connectivity on access point Cisco_ap2:
> config ap ssh enable 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

enable	Enables the Cisco lightweight access point static IP address.
disable	Disables the Cisco lightweight access point static IP address. The access point uses DHCP to get the IP address.
<i>cisco_ap</i>	Cisco lightweight access point name.
<i>ip_address</i>	Cisco lightweight access point IP address
<i>net_mask</i>	Cisco lightweight access point network mask.
<i>gateway</i>	IP address of the Cisco lightweight access point gateway.
add	Adds a domain or DNS server.
domain	Specifies the domain to which a specific access point or all access points belong.
all	All access points.
<i>domain_name</i>	Specifies a domain name.
nameserver	Specifies a DNS server so that a specific access point or all access points can discover the controller using DNS resolution.
<i>dns_ip_address</i>	DNS server IP address.
delete	Deletes a domain or DNS server.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

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.

Examples

This example shows how to configure an access point static IP address:

```
> config ap static-ip enable AP2 1.1.1.1 255.255.255.0 10.1.1.1
```

Related Commands**show sysinfo****config sysname****config ap secondary-base****config ap primary-base**

config ap stats-timer

To set the time in seconds that the Cisco lightweight access point sends its DOT11 statistics to the Cisco wireless LAN controller, use the **config ap stats-timer** command.

config ap stats-timer *period cisco_ap*

Syntax Description	<i>period</i>	Time in seconds from 0 to 65535. A zero value disables the timer.
	<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults	0 (disabled).

Usage Guidelines	A value of 0 (zero) means that the Cisco lightweight access point does not send any DOT11 statistics. The acceptable range for the timer is from 0 to 65535 seconds, and the Cisco lightweight access point must be disabled to set this value.

Examples	This example shows how to set the stats timer to 600 seconds for access point AP2: > 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

syslog_server_IP_address 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

This example shows how to configure a global syslog server for all access points:

```
> 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*

Syntax Description	<i>cisco_ap</i>	Cisco lightweight access point.
	<i>syslog_server_IP_address</i>	Specifies the IP address of the syslog server.

Defaults	0.0.0.0.

Usage Guidelines	By default, the syslog server IP address for each access point is 0.0.0.0, indicating that it is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

Examples	This example shows how to configure a syslog server: > 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

enable	Enables the TCP maximum segment size on an access point.
disable	Disables the TCP maximum segment size on an access point.
cisco_ap	Cisco access point name.
all	Specifies all access points.
size	Maximum segment size, from 536 to 1363 bytes.



Note

If an AP itself is configured with the name ‘all’, then the ‘all access points’ case takes precedence over the AP that is named ‘all’.

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 that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

Examples

This example shows how to enable the TCP MSS on access point Cisco_ap1 with a segment size of 1200 bytes:

```
> 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.

config ap telnet {enable | disable} cisco_ap

Syntax Description	enable	Enables the Telnet connectivity on an access point.
	disable	Disables the Telnet connectivity on an access point.
	<i>cisco_ap</i>	Cisco access point name.

Defaults

None.

Usage Guidelines

The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operation and in the event of a hardware reset.

Examples

This example shows how to enable Telnet connectivity on access point cisco_ap1:

```
> config ap telnet enable cisco_ap1
```

This example shows how to disable Telnet connectivity on access point 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.

config ap tertiary-base *controller_name* *cisco_ap* [*controller_ip_address*]

Syntax Description

<i>controller_name</i>	Name of the 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.

The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operations and in the event of a hardware reset.

Examples

This example shows how to set the access point tertiary wireless LAN controller:

```
> 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

To configure the settings used for downgrading a lightweight access point to an autonomous access point, use the **config ap ftp-downgrade** command.

config ap tftp-downgrade {*tftp_ip_address* | *image_filename* | *ap_name*}

Syntax Description	<i>tftp_ip_address</i>	IP address of the TFTP server.
	<i>image_filename</i>	Filename of the access point image file on the TFTP server.
	<i>ap_name</i>	Access point name.

Defaults	None.

Examples	This example shows how to configure the settings for downgrading access point ap1240_102301: <pre>> config ap tftp-downgrade 10.0.23.8 1238.tar ap1240_102301</pre>

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 the **config ap username** command

```
config ap username user_id password passwd [all | ap_name]
```

Syntax Description

<i>user_id</i>	Administrator username.
<i>passwd</i>	Administrator password.
all	(Optional) Specifies all access points.
<i>ap_name</i>	Name of a specific access point.

Defaults

None.

Examples

This example shows how to assign a username and password to a specific access point:

```
config ap username jack password blue 1a204
```

This example shows how to assign the same username and password to a all access points:

```
config ap username jack password blue all
```

config ap wlan

To enable or disable wireless LAN override for a Cisco lightweight access point radio, use the **config ap wlan** command.

config ap wlan {enable | disable} {802.11a | 802.11b} wlan_id cisco_ap

Syntax Description

enable	Enables the wireless LAN override on an access point.
disable	Disables the wireless LAN override on an access point.
802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
<i>wlan_id</i>	Cisco wireless LAN controller ID assigned to a wireless LAN.
<i>cisco_ap</i>	Cisco lightweight access point name.

Defaults

None.

Examples

This example shows how 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

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

Defaults

None.

Examples

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

```
> config auth-list add mic 00:0b:85:02:0d:20
```

Related Commands

config auth-list delete
config auth-list ap-policy

config auth-list ap-policy

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

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

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

Defaults None.

Examples This example shows how to enable an access point authorization policy:

```
> config auth-list ap-policy authorize-ap enable
```

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

```
> 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	<i>AP_MAC</i> MAC address of a Cisco lightweight access point.
Defaults	None.
Examples	This example shows how to delete an access point entry for MAC address 00:0b:85:02:0d:20: <pre>> config auth-list delete 00:0b:85:02:0d:20</pre>
Related Commands	config auth-list add config auth-list ap-policy

Configure Band-Select Commands

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

config band-select cycle-count

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

config band-select cycle-count *cycle_count*

Syntax Description	<i>cycle_count</i> Value for the cycle count between 1 to 10.
Defaults	None.
Examples	This example shows how to set the probe cycle count for band select to 8: <pre>> config band-select cycle-count 8</pre>
Related Commands	config band-select cycle-threshold config band-select expire config band-select client-rssi

config band-select cycle-threshold

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

config band-select cycle-threshold *cycle_threshold*

Syntax Description	<i>cycle_threshold</i> Value for the cycle threshold between 1 and 1000 milliseconds.
Defaults	None.
Examples	This example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds: <pre>> config band-select cycle-threshold 700</pre>
Related Commands	config band-select cycle-threshold config band-select expire config band-select client-rssi

config band-select expire

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

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

Syntax Description

suppression	Sets the suppression expire to the band select.
dual-band	Sets the dual band expire to the band select.
<i>seconds</i>	- Value for suppression between 10 to 200 seconds. - Value for a dual-band between 10 to 300 seconds.

Defaults

None.

Examples

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

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

Related Commands

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

config band-select client-rssi

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

config band-select client-rssi *client_rssi*

Syntax Description	<i>client_rssi</i> Minimum dBm of a client RSSI to respond to probe between 20 and 90.
Defaults	None.
Examples	This example shows how to set the RSSI threshold for band select to 70: <pre>> config band-select client-rssi 70</pre>
Related Commands	config band-select cycle-threshold config band-select expire config band-select cycle-count

config band-select

To enable client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point, use the **config band-select** command.

config band-select {**probe-response** {**enable** | **disable**} | **cycle-count** *cycles* | **cycle-threshold** *milliseconds* | **expire** {**suppression** *seconds* | **dual-band** *seconds*} | **client-rssi** *dBm*}

Syntax Description

config auth-list	Specifies the command action.
band-select	Specifies the band select mode.
probe-response	Specifies the band selection on the controller.
enable	Enables the band selection on the controller.
disable	Disables the band selection on the controller.
cycle-count <i>cycles</i>	Specifies the number of suppression cycles for a new client, from 1 to 10.
cycle-threshold <i>milliseconds</i>	Specifies the time threshold for a new scanning cycle, from 1 to 1000 milliseconds.
expire	Specifies the expiration time.
suppression <i>seconds</i>	Specifies the suppressed 802.11b/g client expiration time from 10 to 200 seconds.
dual-band <i>seconds</i>	Specifies the dual-band client expiration time from 10 to 300 seconds.
client-rssi <i>dBm</i>	Specifies the minimum RSSI for a client to respond to a probe, from –20 to –90.

Defaults

Band selection is disabled.
 Cycle count is 3.
 Cycle threshold is 200 milliseconds.
 Suppressed 802.11b/g client expiration time is 20 seconds.
 Dual-band client 802.11b/g client expiration time is 60 seconds.
 Minimum RSSI is –80 dBm..

Usage Guidelines

This feature enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point.

You can globally enable band selection on the controller, or you can enable or disable band selection for a particular WLAN (using the [config wlan band-select](#) command), which is useful if you want to disable it for a select group of clients (such as time-sensitive voice clients).



Note

Band-selection-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

Follow these guidelines when using band selection on your controller:

- Band selection can be used only with Cisco Aironet 1140 and 1250 series access points.

- Band selection operates only on access points that are connected to a controller. A hybrid-REAP access point without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

Examples

This example shows how to enable the band selection on the controller:

```
> config band-select probe-response enable
```

This example shows how to configure the number of suppression cycles to 5 for a new client.

```
> config band-select cycle-count 5
```

Related Commands

config wlan band-select

config boot

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

config boot {primary | backup}

Syntax Description	primary	Sets the primary image as active.
	backup	Sets the backup image as active.
Defaults	primary.	
Usage Guidelines	Each Cisco wireless LAN controller can boot off the primary, last-loaded operating system image (OS) or boot off the backup, earlier-loaded OS image.	
Examples	This example shows how to set the primary image as active so that the LAN controller can boot off the primary, last loaded image: > config boot primary	
	This example shows how to set the backup image as active so that the LAN controller can boot off the backup, earlier loaded OS image: > config boot backup	
Related Commands	show boot	

config cdp timer

To configure the Cisco Discovery Protocol (CDP) maximum hold timer, use the **config cdp timer** command.

config cdp timer *seconds*

Syntax Description

<i>seconds</i>	Maximum hold timer value (5 to 254 seconds).

Defaults

None.

Examples

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

```
> config cdp timer 150
```

config certificate

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

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

Syntax Description

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

Defaults

None.

Examples

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

```
> config certificate generate webadmin
```

Creating a certificate may take some time. Do you wish to continue? (y/n)

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

```
> config certificate compatibility
```

Related Commands

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

config certificate lsc

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

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

Syntax Description

enable	Enables LSC certificates on the controller.
disable	Disables LSC certificates on the controller.
ca-server	Specifies the Certificate Authority (CA) server settings.
<i>http://url:port/path</i>	Domain name or IP address of the CA server.
ca-cert	Specifies CA certificate database settings.
add	Obtains a CA certificate from the CA server and adds it to the controller's certificate database.
delete	Deletes a CA certificate from the controller's certificate database.
subject-params	Specifies the device certificate settings.
<i>country state city orgn dept email</i>	Country, state, city, organization, department, and email of the certificate authority.
	Note The common name (CN) is generated automatically on the access point using the current MIC/SSC format <i>Cxxxx-MacAddr</i> , where <i>xxxx</i> is the product number.
other-params	Specifies the device certificate key size settings.
<i>keysize</i>	Value from 384 to 2048 (in bits); the default value is 2048.
ap-provision	Specifies the access point provision list settings.
auth-list	Specifies the provision list authorization settings.
<i>ap_mac</i>	MAC address of access point to be added or deleted from the provision list.
revert-cert	Specifies the number of times the access point attempts to join the controller using an LSC before reverting to the default certificate.
<i>retries</i>	Value from 0 to 255; the default value is 3.
	Note If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate. If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Defaults

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

Usage Guidelines

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

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

Examples

This example shows how to enable the LSC settings:

```
> config certificate lsc enable
```

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

```
> config certificate lsc ca-server http://10.0.0.1:8080/caserver
```

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

```
> config certificate lsc ca-cert add
```

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

```
> config certificate lsc keysize 2048
```

Related Commands

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

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

client_mac_address MAC address of the client.

Defaults

None.

Examples

This example shows how to clear the reporting information of the client MAC address 172.19.28.40:

```
> 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 MAC address of the client.

Defaults

None.

Examples

This example shows how to clear the test results of the client MAC address 172.19.28.40:

```
> config client ccx clear-results 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*

Syntax Description

client_mac_address MAC address of the client.

Defaults

None.

Usage Guidelines

This test does not require the client to use the diagnostic channel.

Examples

This example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the default gateway ping test:

```
> 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*

Syntax Description	<i>client_mac_address</i> MAC address of the client.
Defaults	None.
Usage Guidelines	This test does not require the client to use the diagnostic channel.
Examples	This example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the DHCP test: <pre>> config client ccx dhcp-test 00:E0:77:31:A3:55</pre>
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 Domain Name System (DNS) server IP address ping test, use the **config client ccx dns-ping** command.

config client ccx dns-ping *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Defaults

None.

Usage Guidelines

This test does not require the client to use the diagnostic channel.

Examples

This example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the DNS server IP address ping test:

```
> 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 Domain Name System (DNS) resolution test to the specified hostname, use the **config client ccx dns-resolve** command.

config client ccx dns-resolve *client_mac_address* *host_name*

Syntax Description

<i>client_mac_address</i>	MAC address of the client.
<i>host_name</i>	Hostname of the client.

Defaults

None.

Usage Guidelines

This test does not require the client to use the diagnostic channel.

Examples

This example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the DNS name resolution test to the specified hostname:

```
> 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

client_mac_address MAC address of the client.

Defaults

None.

Examples

This example shows how to send a request to the client 172.19.28.40 to send its capability information:

```
> config client ccx get-client-capability 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 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 MAC address of the client.

Defaults

None.

Examples

This example shows how to send a request to the client 172.19.28.40 to send the manufacturer's information:

```
> 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 MAC address of the client.

Defaults

None.

Examples

This example shows how to send a request to the client 172.19.28.40 to send its current operating parameters:

```
> 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 MAC address of the client.

Defaults

None.

Examples

This example shows how to send a request to the client 172.19.28.40 to send its profile details:

```
> 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	(Optional) Specifies the request to specify the client CCX roaming log.
rsna	(Optional) Specifies the request to specify the client CCX RSNA log.
syslog	(Optional) Specifies the request to specify the client CCX system log.
<i>client_mac_address</i>	MAC address of the client.

Defaults

None.

Examples

This example shows how to specify the request to specify the client CCS system log:

```
> config client ccx log-request 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
```

This example shows how to specify the client CCX roaming log:

```
> config client ccx log-request 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
```

This example shows how to specify the client CCX RSNA log:

```
> config client ccx log-request 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>	MAC address of the client.
<i>message_id</i>	Message type that involves one of the following: • 1—The SSID is invalid. • 2—The network settings are invalid. • 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 connectivity 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 (cont.)</i>	• 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

This example shows how to send a message to the client MAC address 172.19.28.40 with the message user-action-required:

```
> 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>measurement_duration stats_name</i>	Measurement duration in seconds.
	dot11	(Optional) Specifies dot11 counters.
	security	(Optional) Specifies security counters.
	<i>client_mac_address</i>	MAC address of the client.

Defaults	None.

Examples	This example shows how to specify dot11 counter settings:

```
> config client ccx stat-request 1 dot11 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 MAC address of the client.

Defaults

None.

Usage Guidelines

Only one test can be pending at a time.

Examples

This example shows how to send a request to the client 11:11:11:11:11:11 to abort the correct test settings:

```
> 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>	MAC address of the client.
<i>ssid</i>	Network name.
<i>bssid</i>	Basic SSID.
802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
802.11g	Specifies the 802.11g network.
<i>channel</i>	Channel number.

Defaults

None

Examples

This example shows how to send a request to the client MAC address 00:0E:77:31:A3:55 to perform the basic SSID association test:

```
> 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>	MAC address of the client.
<i>profile_id</i>	Test profile name.
<i>bssid</i>	Basic SSID.
802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
802.11g	Specifies the 802.11g network.
<i>channel</i>	Channel number.

Defaults

None.

Examples

This example shows how to send a request to the client to perform the 802.11b test with the profile name profile_01:

```
> config client ccx test-dot1x 172.19.28.40 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>	MAC address of the client.
<i>profile_id</i>	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

This example shows how to send a request to the client to perform the profile redirect test with the profile name profile_01:

```
> config client ccx test-profile 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	<i>MAC</i> Client MAC address.
Defaults	None.
Examples	This example shows how to deauthenticate a client: <pre>> config client deauthenticate 11:11:11:11:11:11</pre>
Related Commands	show client summary show client detail

config client location-calibration

To configure link aggregation, use the **config client location-calibration** command.

config client location-calibration {**enable** *mac_address interval* | **disable** *mac_address*}

Syntax Description	enable	(Optional) Specifies that client location calibration is enabled.
	<i>mac_address</i>	MAC address of the client.
	<i>interval</i>	Measurement interval in seconds.
	disable	(Optional) Specifies that client location calibration is disabled.

Defaults None.

Examples This example shows how to enable the client location calibration for the client 37:15:85:2a with a measurement interval of 45 seconds:

```
> 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

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

Defaults

None.

Examples

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

```
> config coredump enable
```

Related Commands

[config coredump ftp](#)
[config coredump username](#)
[show coredump summary](#)

config coredump ftp

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

config coredump ftp *server_ip_address filename*

Syntax Description	<i>server_ip_address</i>	IP address of the FTP server to which the controller sends its core dump file.
	<i>filename</i>	Name given to the controller core dump file.

Defaults	None.

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

Examples	This example shows how to configure the controller to upload a core dump file named <i>core_dump_controller</i> to an FTP server at network address <i>192.168.0.13</i> :

```
> config coredump ftp 192.168.0.13 core_dump_controller
```

Related Commands	config coredump config coredump username show coredump summary

config coredump username

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

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

Syntax Description

<i>ftp_username</i>	FTP server login username.
<i>ftp_password</i>	FTP server login password.

Defaults

None.

Usage Guidelines

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

Examples

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

```
> config coredump username admin password adminpassword
```

Related Commands

[config coredump](#)
[config coredump ftp](#)
[show coredump summary](#)

config country

To configure the controller's country code, use the **config country** command.

config country *country_code*

Syntax Description

<i>country_code</i>	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. See the related product guide for the most recent country codes and regulatory domains.

You can use the **show country** command to display a list of supported countries.

Examples

This example shows how to configure the controller's country code to DE:

```
> 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

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

Defaults

None.

Examples

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

```
> config custom-web ext-webauth-mode enable
```

Related Commands

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

config custom-web ext-webauth-url

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

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

Syntax Description	<i>URL</i> URL used for web-based client authorization.
Defaults	None.
Examples	This example shows how to configure the complete external web authentication URL <code>http://www.AuthorizationURL.com/</code> for the web-based client authorization: <pre>> config custom-web ext-webauth-url http://www.AuthorizationURL.com/</pre>
Related Commands	<code>config custom-web redirectUrl</code> <code>config custom-web weblogo</code> <code>config custom-web webmessage</code> <code>config custom-web webtitle</code> <code>config custom-web ext-webauth-mode</code> <code>show custom-web</code>

config custom-web ext-webserver

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

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

Syntax Description

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

Defaults

None.

Examples

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

```
> config custom-web ext-webserver add 2 192.23.32.19
```

Related Commands

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

config custom-web redirectUrl

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

config custom-web redirectUrl *URL*

Syntax Description	<i>URL</i> URL that is redirected to the specified address.
Defaults	None.
Examples	This example shows how to configure the URL that is redirected to abc.com: <pre>> config custom-web redirectUrl abc.com</pre>
Related Commands	config custom-web weblogo config custom-web webmessage config custom-web webtitle config custom-web ext-webauth-mode config custom-web ext-webauth-url show custom-web

config custom-web webauth-type

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

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

Syntax Description

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

Defaults

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

Examples

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

```
> config custom-web webauth-type internal
```

Related Commands

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

config custom-web weblogo

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

config custom-web weblogo {enable | disable}

Syntax Description

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

Defaults

None.

Examples

This example shows how to enable the web authentication logo:

```
> config custom-web weblogo enable
```

Related Commands

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

config custom-web webmessage

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

config custom-web webmessage *message*

Syntax Description

<i>message</i>	Message text for web authentication.

Defaults

None.

Examples

This example shows how to configure the message text *Thisistheplace* for webauthentication:

```
> config custom-web webmessage Thisistheplace
```

Related Commands

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

config custom-web webtitle

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

config custom-web webtitle *title*

Syntax Description

<i>title</i>	Custom title text for web authentication.

Defaults

None.

Examples

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

```
> config custom-web webtitle Helpdesk
```

Related Commands

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

config database size

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

config database size *count*

Syntax Description

<i>count</i>	Database size value between 512 and 2040

Defaults

None.

Usage Guidelines

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

Examples

This example shows how to configure 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.

```
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 | ap-ethmac}}
```

Syntax Description

address-pool <i>scope start end</i>	Configures an address range to allocate. You must specify the scope name and the first and last addresses of the address range.
create-scope <i>name</i>	Creates a new DHCP scope. You must specify the scope name. DHCP scope name allows space by using double quote like "scope 003".
default-router <i>scope router_1 [router_2] [router_3]</i>	Configures the default routers for the specified scope and specify the IP address of a router. Optionally, you can specify the IP addresses of secondary and tertiary routers.
delete-scope <i>scope</i>	Deletes the specified DHCP scope.
disable <i>scope</i>	Disables the specified DHCP scope.
dns-servers <i>scope dns1 [dns2] [dns3]</i>	Configures the name servers for the given scope. You must also specify at least one name server. Optionally, you can specify secondary and tertiary name servers.
domain <i>scope domain</i>	Configures the DNS domain name. You must specify the scope and domain names.
enable <i>scope</i>	Enables the specified dhcp scope.
lease <i>scope lease_duration</i>	Configures the lease duration (in seconds) for the specified scope.
netbios-name-server <i>scope wins1 [wins2] [wins3]</i>	Configures the netbios name servers. You must specify the scope name and the IP address of a name server. Optionally, you can specify the IP addresses of secondary and tertiary name servers.
network <i>scope network netmask</i>	Configures the network and netmask. You must specify the scope name, the network address, and the network mask.
opt-82 remote-id	Configures the DHCP Option 82 Remote ID Field Format.
<i>ap_mac</i>	MAC address of the access point to the DHCP option 82 payload.
<i>ap_mac:ssid</i>	MAC address and SSID of the access point to the DHCP option 82 payload.
<i>ap-ethmac</i>	Remote ID format as <AP Ethernet MAC Address> .

Defaults

None.

Usage Guidelines

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

Examples

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

```
> config dhcp lease 003
```

Related Commands

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

config dhcp proxy

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

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

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

Defaults Enabled.

Usage Guidelines Follow these guidelines when you use this command:

- Use the **show dhcp proxy** command to display the status of DHCP proxy handling.
- To enable third-party WGB support, you must enable the passive-client feature on the wireless LAN by entering the **config wlan passive-client enable** command.

Examples This example shows how to disable the DHCP packet modification:

```
> config dhcp proxy disable
```

This example shows how to enable the DHCP BootP broadcast option:

```
> config dhcp proxy disable bootp-broadcast enable
```

Related Commands

- config dhcp
- config dhcp timeout
- config interface dhcp
- config wlan dhcp_server
- config wlan passive-client
- debug dhcp
- debug dhcp service-port
- debug disable-all
- show dhcp
- show dhcp proxy

config dhcp timeout

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

config dhcp timeout *timeout-value*

Syntax Description	<i>timeout-value</i>	The timeout value in the range of 5 to 120 seconds.

Defaults	None.

Examples	This example shows how to set the DHCP timeout to 10 seconds: > config dhcp timeout 10

Related Commands	config dhcp config interface dhcp config wlan dhcp_server config wlan passive-client 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	Configures the exclusion list.
	add	Creates a local exclusion-list entry.
	delete	Deletes a local exclusion-list entry
	description	Specifies the description for an exclusion-list entry.
	<i>MAC</i>	MAC address of the local Excluded entry.
	<i>description</i>	(Optional) The description, up to 32 characters, for an excluded entry.

Defaults None.

Examples

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

```
> config exclusionlist add xx:xx:xx:xx:xx:xx lab
```

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

```
> config exclusionlist delete xx:xx:xx:xx:xx:xx lab
```

Related Commands show exclusionlist

Configure Interface Group Commands

Use the **config interface group** to create and delete an interface group.

config interface group

To add an interface to the existing interface group, use the **config interface group interface** command.

```
config interface group
  {create interface-group-name interface-group-description} |
  {delete interface-group-name} |
  {interface {add | delete} interface-group-name interface-name} |
  {description interface-group-name interface-group-description}
```

Syntax Description

create	Adds a new interface group.
<i>interface-group-name</i>	Interface group's name.
<i>interface-group-description</i>	Interface group's description to be entered within double-quotes. Valid range is up to 32 characters.
delete	Deletes an interface group.
interface	Edits the list of interface represented by the interface group.
add	Adds a new interface to the interface group.
delete	Deletes an interface from the interface group.
description	Configures the description for an interface group.

Defaults

None.

Examples

This example shows how to create a new interface group with the name int-grp-10:

```
> config interface group create int-grp-10 "for wlan1"
```

Configure Guest-LAN Commands

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

config guest-lan

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

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

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

Defaults	None.

Examples	This example shows how to enable a wireless LAN with the LAN ID 16: <pre>> config guest-lan enable 16</pre>

Related Commands	show wlan

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

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

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

Syntax Description

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

Defaults

None.

Examples

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

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

Related Commands

- config guest-lan
- config guest-lan create
- config guest-lan custom-web login_page

config guest-lan custom-web global disable

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

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

Syntax Description

<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

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

```
> config guest-lan custom-web global disable 1
```

Related Commands

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

config guest-lan custom-web login_page

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

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

Syntax Description

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

Defaults

None.

Examples

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

```
> config guest-lan custom-web login_page custompage1 1
```

Related Commands

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

config guest-lan custom-web webauth-type

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

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

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

Defaults Internal.

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

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

Related Commands

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

config guest-lan ingress-interface

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

config guest-lan ingress-interface *guest_lan_id* *interface_name*

Syntax Description

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

Defaults

None.

Examples

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

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

Defaults	None.

Examples	This example shows how to configure an egress interface to transmit guest traffic out of the controller for guest LAN ID 1 and interface name guest01: <pre>> config guest-lan interface 1 guest01</pre>

Related Commands	config ingress-interface guest-lan config guest-lan create

config guest-lan mobility anchor

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

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

Syntax Description

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

Defaults

None.

Examples

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

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

Related Commands

[config mobility group 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 Network Admission Control (NAC) out-of-band support for a guest LAN, use the **config guest-lan nac** command:

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

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

Defaults	None.

Examples	This example shows how to enable the NAC out-of-band support for guest LAN ID 3: <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 | disable | acl | server-precedence} guest_lan_id |
  {web-passthrough {acl | email-input | disable| enable} guest_lan_id}}
```

Syntax Description

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

Defaults

Web authentication.

Examples

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

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

Related Commands

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

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

<i>group_name</i>	Group name.
add	Adds a hybrid-REAP group.
delete	Deletes a hybrid-REAP group.
ap	Adds or deletes an access point to a hybrid-REAP group.
<i>ap-mac</i>	MAC address of the access point.
radius server	Configures a primary or secondary RADIUS server for a hybrid-REAP group.
primary	Designates a RADIUS server as primary server.
secondary	Designates a RADIUS server as secondary server.
<i>server_index</i>	RADIUS server index number.

Defaults

None.

Usage Guidelines

You can add up to 100 clients.

Examples

This example shows how to add a hybrid-REAP group for MAC address 192.12.1.2:

```
> config hreap group 192.12.1.2 add
```

This example shows how to add RADIUS server as a primary server for a hybrid-REAP group with the server index number 1:

```
> config hreap group 192.12.1.2 radius server add primary 1
```

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

enable	Enables the access point to choose the controller with the least latency when joining.
disable	Disables the access point to choose the controller with the least latency when joining.
<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 the discovery request and discovery response and joins the Cisco 5500 Series Controller that responds first.

Examples

This example shows how to enable the access point to choose the controller with the least latency when joining:

```
> 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	enable	Enables the OfficeExtend mode for an access point.
	disable	Disables the OfficeExtend mode for an access point.
	clear-personalssid-config	Clears 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 by using the **config rogue detection** {enable | disable} {*cisco_ap* | all} command.

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 by using the **config ap link-encryption** {enable | disable} {*cisco_ap* | all} command.

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 by using the **config ap telnet** {enable | disable} *cisco_ap* or **config ap ssh** {enable | disable} *cisco_ap* command.

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 by using the **config ap link-latency** {enable | disable} {*cisco_ap* | all} command.

Examples This example shows how to enable the office-extend mode for the access point Cisco_ap:

```
> config hreap office-extend enable Cisco_ap
```

This example shows how to clear only the access point's personal SSID for the access point 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

ap-manager	Configures the access point manager interface.
management	Configures the management interface.
<i>interface_name</i>	Interface name.
<i>ACL</i>	ACL name up to 32 alphanumeric characters.
none	Specifies none.

Defaults

None.

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

Examples

This example shows how to configure an access control list with a value None:

```
> config interface acl management none
```

Related Commands

show interface

config interface address

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

config interface address

```
{ap-manager IP_address netmask gateway |  
management IP_address netmask gateway |  
service-port IP_address netmask |  
virtual IP_address |  
interface-name interface-name IP_address netmask gateway}
```

Syntax Description

ap-manager	Specifies the access point manager interface.
<i>IP_address</i>	IP address.
<i>netmask</i>	Network mask.
<i>gateway</i>	IP address of the gateway.
management	Specifies the management interface.
service-port	Specifies the out-of-band service port interface.
virtual	Specifies the virtual gateway interface.
interface-name	Specifies the interface identified by the <i>interface-name</i> parameter.
<i>interface-name</i>	Interface name.

Defaults

None.

Usage Guidelines

For Cisco 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

This example shows how to configure an access point manager interface with IP address 10.109.15.7, network mask 255.255.0.0, and gateway address 10.109.15.1:

```
> 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 {**management** | *interface_name*} {**enable** | **disable**}

Syntax Description

management	Specifies the management interface.
<i>interface_name</i>	Dynamic interface name.
enable	Enables access point manager features on a dynamic interface.
disable	Disables 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 Cisco 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

This example shows how to disable an access point manager myinterface:

```
> 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

<i>interface_name</i>	Interface name.
<i>vlan-id</i>	VLAN identifier.

Defaults

None.

Examples

This example shows how to create a dynamic interface with the interface named lab2 and VLAN ID 6:

```
> 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	<i>interface-name</i> Interface name.
Defaults	None.
Examples	This example shows how to delete a dynamic interface named VLAN501: > 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.
primary	(Optional) Specifies the primary DHCP server.
<i>dhcp_server</i>	IP address of the server.
secondary	(Optional) Specifies the secondary DHCP server.
option-82	(Optional) Configures DHCP Option 82 on the interface.
enable	(Optional) Enables the feature.
disable	(Optional) Disables the feature.
management	Configures the management interface.
service-port	Specifies the DHCP for the out-of-band service port.
dynamic-interface	Specifies the interface name and the primary DHCP server. Optionally, you can also enter the address of the alternate DHCP server.

Defaults

None.

Examples

This example shows how to configure ap-manager server with the primary DHCP server 10.21.15.01 and secondary DHCP server 10.21.15.25:

```
> config interface dhcp ap-manager server-1 10.21.15.01 server-2 10.21.15.25
```

This example shows how to configure DHCP option 82 on the ap-manager:

```
> config interface dhcp ap-manager option-82 enable
```

This example shows how to enable the DHCP for the out-of-band service port:

```
> 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 group

To configure interface groups, use the **config interface group** command.

```
config interface group {{create | delete} interface_group_name description_details} | {description  
interface_group_name description_details} | {interface {add | delete} interface_group_name  
interface_name}}
```

Syntax Description

create	Adds a new interface group.
delete	Deletes an interface group.
<i>interface_group_name</i>	Interface group name that can be up to 32 alphanumeric characters. Note To display details of all interface groups, use the show interface group summary command.
description	Adds a description to the specified interface group.
<i>description_details</i>	Description of the interface group to be entered. The description can be up to 32 alphanumeric characters within double-quotes, including the double-quotes.
interface	Edits the list of interfaces in an interface group.
add	Adds a new interface to an interface group.
delete	Deletes an interface from an interface group.
<i>interface_name</i>	Interface name that can be up to 32 alphanumeric characters. Note To display details of all the interfaces, use the show interface summary command.

Defaults

None.

Examples

This example shows how to create a new interface group and add a description to the group:

```
> config interface group create mygroup1 "My interface group"
```

This example shows how to delete an interface group:

```
> config interface group delete mygroup1
```

This example shows how to add an interface to an interface group:

```
> config interface group interface add mygroup1 myinterface1
```

Related Commands

```
show interface group summary  
show interface summary
```

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	<i>interface_name</i>	Interface name.
	enable	Enables the guest LAN.
	disable	Disables the guest LAN.

Defaults	None.

Examples	This example shows how to enable the guest LAN feature on the interface named myinterface: <pre>> config interface guest-lan myinterface enable</pre>

Related Commands	config guest-lan create

config interface hostname

To configure the Domain Name System (DNS) hostname of the virtual gateway interface, use the **config interface hostname** command.

config interface hostname virtual *DNS_host*

Syntax Description

virtual	Specifies 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.
<i>DNS_host</i>	DNS hostname.

Defaults

This example shows how to configure virtual gateway interface to use the specified virtual address of the fully qualified DNS hostname DNS_Host:

```
> config interface hostname virtual DNS_Host
```

Related Commands

show interface

config interface nat-address

To deploy your Cisco 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

management	Specifies the management interface.
dynamic-interface <i>interface_name</i>	Specifies the dynamic interface name.
enable	Enables one-to-one mapping NAT on the interface.
disable	Disables one-to-one mapping NAT on the interface.
<i>public_IP_address</i>	External NAT IP address.

Defaults

None.

Usage Guidelines

These NAT commands can be used only on Cisco 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, where 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

This example shows how to enable one-to-one mapping NAT on the management interface:

```
> config interface nat-address management enable
```

This example shows how to set the external NAT IP address 10.10.10.10 on the management interface:

```
> 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

management	Specifies the management interface.
<i>interface_name</i>	Interface name.
<i>primary_port</i>	Primary physical port number.
<i>secondary_port</i>	(Optional) Secondary physical port number.

Defaults

None.

Usage Guidelines

You can use the **management** option for all controllers except the Cisco 5500 Series Controllers.

Examples

This example shows how to configure the LAb02 interface's primary port number to 3:

```
> 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	<i>interface-name</i>	Interface's name.
	<i>vlan_id</i>	VLAN identifier.
	Note Enter 0 to disable quarantine processing.	

Defaults None.

Examples This example shows how to configure a quarantine VLAN on the quarantine interface with the VLAN ID 10:

```
> 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	ap-manager	Configures the access point manager interface.
	management	Configures the management interface.
	<i>interface_name</i>	Interface name.
	<i>vlan</i>	VLAN identifier.

Defaults None.

Examples This example shows how to configure VLAN ID 10 on the management interface:

```
> 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	add	Adds a new known access point Entry.
	alert	Generates a trap upon detection of the access point.
	delete	Deletes an existing known access point entry.
	<i>MAC</i>	MAC address of the known Cisco lightweight access point.

Defaults	None.

Examples	This example shows how to add a new access point entry ac:10:02:72:2f:bf on a known access point: <pre>> config known ap add ac:10:02:72:2f:bf 12</pre>

Related Commands	config ap

config lag

To enable or disable link aggregation (LAG), use the **config lag** command.

config lag {enable | disable}

Syntax Description

enable	Enables the link aggregation (LAG) settings.
disable	Disables the link aggregation (LAG) settings.

Defaults

None.

Examples

This example shows how to enable LAG settings:

```
> 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.
```

This example shows how to disable LAG settings:

```
> 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 the 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

This example shows how to enable LDAP server index 10:

```
> config ldap enable 10
```

Related Commands

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

config ldap add

To configure a Lightweight Directory Access Protocol (LDAP) server, use the **config ldap add** command.

config ldap add *index server_ip_address port user_base user_attr user_type*

Syntax Description

<i>index</i>	LDAP server index.
<i>server_ip_address</i>	IP address of the LDAP server.
<i>port</i>	Port number.
<i>user_base</i>	Distinguished name for the subtree that contains all of the users.
<i>user_attr</i>	Attribute that contains the username.
<i>user_type</i>	ObjectType that identifies the user.

Defaults

None.

Examples

This example shows how to configure a LDAP server with the index10, server IP address 10.31.15.45, port number 2:

```
> 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 Lightweight Directory Access Protocol (LDAP) server, use the **config ldap simple-bind** command.

```
config ldap simple-bind { anonymous index | authenticated index username username password
password }
```

Syntax Description

anonymous	Allows anonymous access to the LDAP server.
<i>index</i>	LDAP server index.
authenticated	Specifies that a username and password be entered to secure access to the LDAP server.
<i>username</i>	Username for the authenticated bind method.
<i>password</i>	Password for the authenticated bind method.

Defaults

The default bind method is **anonymous**.

Examples

This example shows how to configure the local authentication bind method that allows anonymous access to the LDAP server:

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

Defaults

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

The listener is **disabled** by default.

Notify is **disabled** by default.

The default maximum number of sessions is **9**.

The default maximum message size is **0**.

Usage Guidelines

If your network contains various Cisco licensed devices, you might consider using the CLM to manage all of the licenses using a single application. CLM is a secure client/server application that manages Cisco software licenses network wide.

The license agent is an interface module that runs on the controller and mediates between CLM and the controller's licensing infrastructure. CLM can communicate with the controller using various channels, such as HTTP, Telnet, and so on. If you want to use HTTP as the communication method, you must enable the license agent on the controller.

The license agent receives requests from the CLM and translates them into license commands. It also sends notifications to the CLM. It uses XML messages over HTTP or HTTPS to receive the requests and send the notifications. For example, if the CLM sends a **license clear** command, the agent notifies the CLM after the license expires.

**Note**

You can download the CLM software and access user documentation at this URL:
<http://www.cisco.com/en/US/products/ps7138/index.html>

Examples

This example shows how to authenticate the default license agent settings:

```
> config license agent default authenticate
```

This example shows how to configure the license agent with the number of maximum sessions allowed as 5:

```
> config license agent max-session 5
```

Related Commands

[license install](#)
[show license agent](#)
[clear license agent](#)

config license boot

To specify the license level to be used on the next reboot of the Cisco 5500 Series Controller, use the **config license boot** command.

config license boot {base | wplus | auto}

Syntax Description

base	Specifies base boot level.
wplus	Specifies wplus boot level.
auto	Specifies auto boot 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

This example shows how to set the license boot settings to wplus:

```
> config license 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 {**window** *client_count* | **status** {**enable** | **disable**} | **denial** *denial_count*}

Syntax Description

window	Specifies the aggressive load balancing client window.
<i>client_count</i>	Sets the aggressive load balancing client window with the number of clients from 1 to 20.
status	Sets the load balancing status.
enable	Enables load balancing feature.
disable	Disables load balancing feature.
denial	Specifies the number of association denials during load balancing.
<i>denial_count</i>	Sets 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

This example shows how to enable the aggressive load-balancing settings:

```
> 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 Extensible Authentication Protocol (EAP) after any pair of configured RADIUS servers fails, use the **config local-auth active-timeout** command.

config local-auth active-timeout *timeout*

Syntax Description

<i>timeout</i>	Timeout measured in seconds. The valid range is 1 to 3600.

Defaults

This command has a default of 100 seconds.

Examples

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

```
> config local-auth active-timeout 500
```

Related Commands

[clear stats local-auth](#)
[config local-auth eap-profile](#)
[config local-auth method fast](#)
[config local-auth user-credentials](#)
[debug aaa local-auth](#)
[show local-auth certificates](#)
[show local-auth config](#)
[show local-auth statistics](#)

config local-auth eap-profile

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

```
config local-auth eap-profile {{add | delete} profile_name |
    cert-issuer {cisco | vendor} |
    method [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

add	(Optional) Specifies that an EAP profile or method is being added.
delete	(Optional) Specifies that an EAP profile or method is being deleted.
<i>profile_name</i>	EAP profile name (up to 63 alphanumeric characters). Do not include spaces within a profile name.
cert-issuer	(For use with EAP-TLS, PEAP, or EAP-FAST with certificates) Specifies the issuer of the certificates that will be sent to the client. The supported certificate issuers are Cisco or a third-party vendor.
Cisco	Specifies the Cisco certificate issuer.
Vendor	Specifies the third-party vendor.
method	Configures an EAP profile method.
<i>method</i>	EAP profile method name. The supported methods are leap, fast, tls, and peap.
local-cert	(For use with EAP-FAST) Specifies whether the device certificate on the controller is required for authentication.
enable	Specifies that the parameter is enabled.
disable	Specifies that the parameter is disabled.
client-cert	(For use with EAP-FAST) Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.
peer-verify	Configures the peer certificate verification options.
ca-issuer	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the incoming certificate from the client is to be validated against the Certificate Authority (CA) certificates on the controller.
cn-verify	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates' CN on the controller.
date-valid	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.

Defaults

None.

Examples

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

```
> config local-auth eap-profile add FAST01
```

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

```
> config local-auth eap-profile method add fast FAST01
```

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

```
> config local-auth eap-profile method fast cert-issuer cisco
```

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

```
> config local-auth eap-profile method fast peer-verify ca-issuer enable
```

Related Commands

[config local-auth active-timeout](#)
[config local-auth method fast](#)
[config local-auth user-credentials](#)
[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

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

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

Syntax Description

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

Defaults

None.

Examples

This example shows how to disable the controller to allows anonymous provisioning:

```
> config local-auth method fast anon-prov disable
```

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

```
> config local-auth method fast authority-id 0125631177
```

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

```
> config local-auth method fast pac-ttl 10
```

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

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

Syntax Description

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

Defaults

None.

Usage Guidelines

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

Examples

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

```
> config local-auth user-credentials local lda
```

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

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

add	Adds a location element.
<i>location</i>	Location element name.
<i>description</i>	Element description. Optional with the add command, and required with the description command.
delete	Deletes a location element.
enable	Enables the access point location-based overrides.
disable	Disables the access point location-based overrides.
algorithm	Note We recommend that you do not use or modify the config location algorithm command. It is set to optimal default values. Configures the algorithm used to average RSSI and SNR values.
simple	Specifies a faster algorithm that requires low CPU overhead but provides less accuracy.
rssi-average	Specifies a more accurate algorithm but requires more CPU overhead.
rssi-half-life	Note We recommend that you do not use or modify the config location rssi-half-life command. It is set to optimal default values. Configures the half-life when averaging two RSSI readings.
expiry	Note We recommend that you do not use or modify the config location expiry command. It is set to optimal default values. Configures the timeout for RSSI values.
client	(Optional) Specifies the parameter applies to client devices.
calibrating-client	(Optional) Specifies the parameter is used for calibrating client devices.
tags	(Optional) Specifies the parameter applies to radio frequency identification (RFID) tags.
rogue-aps	(Optional) Specifies the parameter applies to rogue access points.
<i>seconds</i>	Time value (0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, 300 seconds).
notify-threshold	Note We recommend that you do not use or modify the config location notify-threshold command. It is set to optimal default values. NMSP notification threshold for RSSI measurements.
<i>threshold</i>	Threshold parameter. The range is 0 to 10 dB, and the default value is 0 dB.
interface-mapping	Adds or deletes a new location, wireless LAN, or interface mapping element.

<i>wlan_id</i>	WLAN identification name.
<i>interface_name</i>	Name of interface to which mapping element applies.
plm	Specifies the path loss measurement (S60) request for normal clients or calibrating clients.
client	Specifies normal, noncalibrating clients.
<i>burst_interval</i>	Burst interval. The range is 1 to 3600 seconds, and the default value is 60 seconds.
calibrating	Specifies calibrating clients.
uniband	Specifies the associated 802.11a or 802.11b/g radio (uniband).
multiband	Specifies the associated 802.11a/b/g radio (multiband).

Defaults

See the “Syntax Description” section for default values of individual arguments and keywords.

Examples

This example shows how to specify the **simple** algorithm for averaging RSSI and SNR values on a location-based controller:

```
> config location algorithm simple
```

Related Commands

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

config logging buffered

To set the severity level for logging messages to the controller buffer, use the **config logging buffered** command.

config logging buffered *security_level*

Syntax Description

security_level

Security level. Choose one of the following:

- emergencies—Severity level 0
- alerts—Severity level 1
- critical—Severity level 2
- errors—Severity level 3
- warnings—Severity level 4
- notifications—Severity level 5
- informational—Severity level 6
- debugging—Severity level 7

Defaults

None.

Examples

This example shows how to set the controller buffer severity level for logging messages to 4:

```
> config logging buffered 4
```

Related Commands

[config logging syslog facility](#)
[config logging syslog level](#)
[show logging](#)

config logging console

To set the severity level for logging messages to the controller console, use the **config logging console** command.

config logging console *security_level*

Syntax Description	<i>security_level</i>	Severity level. Choose one of the following: - emergencies—Severity level 0 - alerts—Severity level 1 - critical—Severity level 2 - errors—Severity level 3 - warnings—Severity level 4 - notifications—Severity level 5 - informational—Severity level 6 - debugging—Severity level 7
Defaults	None.	
Examples	This example shows how to set the controller console severity level for logging messages to 3: > config logging console 3	
Related Commands	config logging syslog facility config logging syslog level show logging	

config logging debug

To save debug messages to the controller buffer, the controller console, or a syslog server, use the **config logging debug** command.

config logging debug {buffered | console | syslog} {enable | disable}

Syntax Description

buffered	Saves debug messages to the controller buffer.
console	Saves debug messages to the controller console.
syslog	Saves debug messages to the syslog server.
enable	Enables logging of debug messages.
disable	Disables logging of debug messages.

Command Default

The **console** command is enabled,
The **buffered** and **syslog** commands are disabled.

Examples

This example shows how to save the debug messages to the controller console:

```
> config logging debug console enable
```

Related Commands

show logging

config logging fileinfo

To cause the controller to include information about the source file in the message logs or to prevent the controller from displaying this information, use the **config logging fileinfo** command.

config logging fileinfo {enable | disable}

Syntax Description

enable	Includes information about the source file in the message logs.
disable	Prevents the controller from displaying information about the source file in the message logs.

Defaults

None.

Examples

This example shows how to enable the controller to include information about the source file in the message logs:

```
> config logging fileinfo enable
```

Related Commands

show logging

config logging procinfo

To cause the controller to include process information in the message logs or to prevent the controller from displaying this information, use the **config logging procinfo** command.

config logging procinfo {enable | disable}

Syntax Description

enable	Includes process information in the message logs.
disable	Prevents the controller from displaying process information in the message logs.

Defaults

None.

Examples

This example shows how to enable the controller to include the process information in the message logs:

```
> config logging procinfo enable
```

Related Commands

show logging

config logging traceinfo

To cause the controller to include traceback information in the message logs or to prevent the controller from displaying this information, use the **config logging traceinfo** command.

config logging traceinfo {enable | disable}

Syntax Description	enable	Includes traceback information in the message logs.
	disable	Prevents the controller from displaying traceback information in the message logs.

Defaults None.

Examples This example shows how to disable the controller to include the traceback information in the message logs:

```
> config logging traceinfo disable
```

Related Commands **show logging**

config logging syslog host

To configure a remote host for sending syslog messages, use the **config logging syslog host** command.

config logging syslog host {*host_IP_address*}

Syntax Description	<i>host_IP_address</i> IP address for the remote host.
Defaults	None.
Usage Guidelines	To remove a remote host that was configured for sending syslog messages, enter the config logging syslog host <i>host_IP_address</i> delete command.
Examples	This example shows how to configure a remote host 10.92.125.52 for sending the syslog messages: <pre>> config logging syslog host 10.92.125.51</pre>
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	<i>facility_code</i>	Facility code. Choose one of the following: • authorization—Authorization system. Facility level—4. • auth-private—Authorization system (private). Facility level—10. • cron—Cron/at facility. Facility level—9. • daemon—System daemons. Facility level—3. • ftp—FTP daemon. Facility level—11. • kern—Kernel. Facility level—0. • local0—Local use. Facility level—16. • local1—Local use. Facility level—17. • local2—Local use. Facility level—18. • local3—Local use. Facility level—19. • local4—Local use. Facility level—20. • local5—Local use. Facility level—21. • local6—Local use. Facility level—22. • local7—Local use. Facility level—23. • lpr—Line printer system. Facility level—6. • mail—Mail system. Facility level—2. • news—USENET news. Facility level—7. • sys12—System use. Facility level—12. • sys13—System use. Facility level—13. • sys14—System use. Facility level—14. • sys15—System use. Facility level—15. • syslog—The syslog itself. Facility level—5. • user—User process. Facility level—1. • uucp—UNIX-to-UNIX copy system. Facility level—8.

Defaults None.

Examples This example shows how to set the facility for outgoing syslog messages to authorization:

```
> config logging syslog facility authorization
```

Related Commands

config logging syslog host
config logging syslog level
show logging

config logging syslog level

To set the severity level for filtering syslog messages to the remote host, use the **config logging syslog level** command.

config logging syslog level *severity_level*

Syntax Description

severity_level

severity level. Choose one of the following:

- emergencies—Severity level 0
 - alerts—Severity level 1
 - critical—Severity level 2
 - errors—Severity level 3
 - warnings—Severity level 4
 - notifications—Severity level 5
 - informational—Severity level 6
 - debugging—Severity level 7
-

Defaults

None.

Examples

This example shows how to set the severity level for syslog messages to 3:

```
> config logging syslog level 3
```

Related Commands

config logging syslog host
config logging syslog facility
show logging

config login session close

To close all active Telnet session(s), use the **config login session close** command.

config login session close {*session_id* | **all**}

Syntax Description

<i>session_id</i>	ID of the session to close.
all	Closes all Telnet sessions.

Defaults

None.

Examples

This example shows how to close all active Telnet sessions:

```
> config login session close all
```

Related Commands

[show login session](#)

config lsc mesh

To enable the locally significant certificate (LSC) on mesh access points, use the **config lsc mesh** command.

config lsc mesh {enable | disable}

Syntax Description

enable	Enables LSC on mesh access points.
disable	Disables LSC on mesh access points.

Defaults

None.

Examples

This example shows how to enable LSC on mesh access point:

```
> config lsc mesh enable
```

Related Commands

[show login session](#)

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 macfilter** command.

```
config macfilter {add client_MAC wlan_id [interface_name] [description] [macfilter_IP] |  
                  delete client_MAC}
```

Syntax Description	add	Adds a MAC filter entry on the controller.
	client_MAC	Client MAC address.
	wlan_id	Wireless LAN identifier with which the MAC filter entry should associate. A zero value associates the entry with any wireless LAN.
	interface_name	Name of the interface. Enter 0 to specify no interface.
	description	(Optional) Short description of the interface (up to 32 characters) in double quotes. Note A description is mandatory if <i>macfilterIP</i> is specified.
	macfilter_IP	(Optional) IP address of the local MAC filter database.
	delete	Deletes 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	This example shows how to add a MAC filter entry 00:E0:77:31:A3:55 with the wireless LAN ID 1, interface name labconnect, and MAC filter IP 10.92.125.51 on the controller:

```
> config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

Related Commands	show macfilter config macfilter ip-address

config macfilter description

To add a description to a MAC filter, use the **config macfilter description** command.

config macfilter description *MAC description*

Syntax Description	<i>MAC</i>	Client MAC address.
	<i>description</i>	(Optional) Description within double quotes (up to 32 characters).

Defaults	None.

Examples	This example shows how to set the description MAC filter 01 to MAC address 11:11:11:11:11:11: <pre>> config macfilter description 11:11:11:11:11:11 "MAC Filter 01"</pre>

Related Commands	show macfilter

config macfilter interfac

To create a MAC filter client interface, use the **config macfilter interface** command.

config macfilter interface *MAC interface*

Syntax Description	<i>MAC</i>	Client MAC address.
	<i>interface</i>	Interface name. A value of zero is equivalent to no name.
Defaults	None.	
Examples	This example shows how to create a MAC filter interface Lab01 on client 11:11:11:11:11:11 : > 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 **config macfilter ip-address** command.

config macfilter ip-address *MAC_address IP_address*

Syntax Description

<i>MAC_address</i>	Client MAC address.
<i>IP_address</i>	IP address for a specific MAC address in the local MAC filter database.

Defaults

None.

Examples

This example shows how to specify IP address **10.92.125.51** for a MAC **00:E0:77:31:A3:55** in the local **MAC filter database**:

```
> 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

none	Disables the delimiters (for example, xxxxxxxxxx).
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).

Defaults

The default delimiter is hyphen.

Examples

This example shows how 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
```

This example shows how 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
```

This example shows how 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

To configure the Cisco wireless LAN controller for compatibility with selected RADIUS servers, use the **config macfilter radius-compact** command.

```
config macfilter radius-compat {Cisco | free | other}
```

Syntax Description	Cisco	Configures the Cisco ACS compatibility mode (password is the MAC address of the server).
	free	Configures the Free RADIUS server compatibility mode (password is secret).
	other	Configures for other server behaviors (no password is necessary).

Defaults Other.

Examples This example shows how to configure the Cisco ACS compatibility mode to “other”:
> 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	<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	This example shows how to modify client wireless LAN ID 2 for a MAC filter 11:11:11:11:11:11: <pre>> config macfilter wlanid 11:11:11:11:11:11 2</pre>

Related Commands	show macfilter show wlan

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	<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	This example shows how to modify client wireless LAN ID 2 for a MAC filter 11:11:11:11:11:11: <pre>> config macfilter wlanid 11:11:11:11:11:11 2</pre>

Related Commands	show macfilter show wlan

config remote-lan

To configure a remote LAN, use the **config remote-lan** command.

config remote-lan {enable | disable} remote-lan-id | all

Syntax Description	enable	Enables a remote LAN.
	disable	Disables a remote LAN.
	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
	all	Configures all wireless LANs.

Defaults None.

Examples This example shows how to enable a remote LAN with ID 2:

```
> config remote-lan enable 2
```

Related Commands [show remote-lan](#)

config remote-lan aaa-override

To configure user policy override through AAA on a remote LAN, use the **config remote-lan aaa-override** command.

```
config remote-lan aaa-override {enable | disable} remote-lan-id
```

Syntax Description	enable	Enables user policy override through AAA on a remote LAN.
	disable	Disables user policy override through AAA on a remote LAN.
	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.

Defaults None.

Examples This example shows how to enable user policy override through AAA on a remote LAN where the remote LAN ID is 2:

```
> config remote-lan aaa-override enable 2
```

Related Commands [show remote-lan](#)

config remote-lan acl

To specify an access control list (ACL) for a remote LAN, use the **config remote-lan acl** command.

config remote-lan acl *remote-lan-id* *acl_name*

Syntax Description	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
	<i>acl_name</i>	ACL name.
	Note	Use the show acl summary command to know the ACLs available.

Defaults	None.

Examples	This example shows how to specify ACL1 for a remote LAN whose ID is 2: <pre>> config remote-lan acl 2 ACL1</pre>

Related Commands	show remote-lan

config remote-lan create

To configure a new remote LAN connection, use the **config remote-lan create** command.

config remote-lan create *remote-lan-id name*

Syntax Description	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
	<i>name</i>	Remote LAN name. Valid values are up to 32 alphanumeric characters.

Defaults	None.

Examples	This example shows how to configure a new remote LAN, MyRemoteLAN, with the LAN ID as 3: <pre>> config remote-lan create 3 MyRemoteLAN</pre>

Related Commands	show remote-lan

config remote-lan custom-web

To configure web authentication for a remote LAN, use the **config remote-lan custom-web** command.

```
config remote-lan custom-web
  {ext-webauth-url URL remote-lan-id} |
  {global {enable | disable} remote-lan-id } |
  {login-page page-name remote-lan-id} |
  {loginfailure-page {page-name | none} remote-lan-id} |
  {logout-page {page-name | none} remote-lan-id} |
  {webauth-type {internal | customized | external} remote-lan-id}
```

Syntax Description

ext-webauth-url	Configures an external web authentication URL.
<i>URL</i>	Web authentication URL for the Login page.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
global	Configures the global status for the remote LAN.
enable	Enables the global status for the remote LAN.
disable	Disables the global status for the remote LAN.
login-page	Configures a login page.
<i>page-name</i>	Login page name.
none	Configures no login page.
logout-page	Configures a logout page.
none	Configures no logout page.
<i>webauth-type</i>	Configures the web authentication type for the remote LAN.
internal	Displays the default login page.
customized	Displays a downloaded login page.
external	Displays a login page that is on an external server.
<i>name</i>	Remote LAN name. Valid values are up to 32 alphanumeric characters.

Defaults

None.

Usage Guidelines

Follow these guidelines when you use the **config remote-lan custom-web** command:

- When you configure the external Web-Auth URL, do the following:
 - Ensure that Web-Auth or Web-Passthrough Security is in enabled state. To enable Web-Auth, use the **config remote-lan security web-auth enable** command. To enable Web-Passthrough, use the **config remote-lan security web-passthrough enable** command.
 - Ensure that the global status of the remote LAN is in disabled state. To enable the global status of the remote LAN, use the **config remote-lan custom-web global disable** command.
 - Ensure that the remote LAN is in disabled state. To disable a remote LAN, use the **config remote-lan disable** command.
- When you configure the Web-Auth type for the remote LAN, do the following:

- When you configure a customized login page, ensure that you have a login page configured. To configure a login page, use the **config remote-lan custom-web login-page** command.
- When you configure an external login page, ensure that you have configured preauthentication ACL for external web authentication to function.

Examples

This example shows how to configure an external web authentication URL for a remote LAN with ID 3:

```
> config remote-lan custom-web ext-webauth-url http://www.AuthorizationURL.com/ 3
```

This example shows how to enable the global status of a remote LAN with ID 3:

```
> config remote-lan custom-web global enable 3
```

This example shows how to configure the login page for a remote LAN with ID 3:

```
> config remote-lan custom-web login-page custompage1 3
```

This example shows how to configure a web authentication type with the default login page for a remote LAN with ID 3:

```
> config remote-lan custom-web webauth-type internal 3
```

Related Commands

[show remote-lan](#)

config remote-lan delete

To delete a remote LAN connection, use the **config remote-lan delete** command.

config remote-lan delete *remote-lan-id*

Syntax Description	<i>remote-lan-id</i> Remote LAN identifier. Valid values are between 1 and 512.
Defaults	None.
Examples	This example shows how to delete a remote LAN with ID 3: > config remote-lan delete 3
Related Commands	show remote-lan

config remote-lan dhcp_server

To configure a dynamic host configuration protocol (DHCP) server for a remote LAN, use the **config remote-lan dhcp_server** command.

config remote-lan dhcp_server *remote-lan-id* *ip_address*

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>ip_address</i>	IP Address of the DHCP server.

Defaults

None.

Examples

This example shows how to configure a DHCP server for a remote LAN with ID 3:

```
> config remote-lan dhcp_server 3 209.165.200.225
```

Related Commands

[show remote-lan](#)

config remote-lan exclusionlist

To configure the exclusion list timeout on a remote LAN, use the **config remote-lan exclusionlist** command.

config remote-lan exclusionlist *remote-lan-id* {seconds | **disabled** | **enabled**}

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
seconds	Exclusion list timeout in seconds. A value of 0 requires an administrator override.
disabled	Disables exclusion listing.
enabled	Enables exclusion listing.

Defaults

None.

Examples

This example shows how to configure the exclusion list timeout to 20 seconds on a remote LAN with ID 3:

```
> config remote-lan exclusionlist 3 20
```

Related Commands

[show remote-lan](#)

config remote-lan interface

To configure an interface for a remote LAN, use the **config remote-lan interface** command.

```
config remote-lan interface remote-lan-id interface_name
```

Syntax Description	remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
	interface_name	Interface name.
	Note Interface name should not be in upper case characters.	

Defaults None.

Examples This example shows how to configure an interface myinterface for a remote LAN with ID 3:
> config remote-lan interface 3 myinterface

Related Commands [show remote-lan](#)

config remote-lan ldap

To configure a remote LAN's LDAP servers, use the **config remote-lan ldap** command.

config remote-lan ldap {add | delete} remote-lan-id index

Syntax Description	add	Adds a link to a configured LDAP server (maximum of three).
	delete	Deletes a link to a configured LDAP server.
	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
	<i>index</i>	LDAP server index.

Defaults None.

Examples This example shows how to add an LDAP server with the index number 10 for a remote LAN with ID 3:

```
> config remote-lan ldap add 3 10
```

Related Commands [show remote-lan](#)

config remote-lan mac-filtering

To configure MAC filtering on a remote LAN, use the **config remote-lan mac-filtering** command.

config remote-lan mac-filtering {enable | disable} remote-lan-id

Syntax Description	enable	Enables MAC filtering on a remote LAN.
	disable	Disables MAC filtering on a remote LAN.
	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.

Defaults	Enabled.

Examples	This example shows how to disable MAC filtering on a remote LAN with ID 3: <pre>> config remote-lan mac-filtering disable 3</pre>

Related Commands	show remote-lan

config remote-lan max-associated-clients

To configure the maximum number of client connections on a remote LAN, use the **config remote-lan max-associated-clients** command.

config remote-lan max-associated-clients *remote-lan-id* *max-clients*

Syntax Description	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
	<i>max-clients</i>	Configures the maximum number of client connections on a remote LAN.

Defaults None.

Examples This example shows how to configure 10 client connections on a remote LAN with ID 3:
> **config remote-lan max-client-associations 3 10**

Related Commands [show remote-lan](#)

config remote-lan radius_server

To configure the Remote Authentication Dial In User Service (RADIUS) servers on a remote LAN, use the **config remote-lan radius_server** command.

config remote-lan radius_server

```
{acct {add | delete} remote-lan-id server-index | {enable | disable} remote-lan-id} |
{auth {add | delete} remote-lan-id server-index | {enable | disable} remote-lan-id} |
{overwrite-interface {enable | disable} remote-lan-id}
```

Syntax Description

acct	Configures a RADIUS accounting server.
add	Adds a link to a configured RADIUS server.
delete	Deletes a link to a configured RADIUS server.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>server-index</i>	RADIUS server index.
enable	Enables RADIUS accounting for this remote LAN.
disable	Disables RADIUS accounting for this remote LAN.

Defaults

None.

Examples

This example shows how to enable RADIUS accounting for a remote LAN with ID 3:

```
> config remote-lan acct enable 3
```

Related Commands

[show remote-lan](#)

config remote-lan security

To configure security policy for a remote LAN, use the **config remote-lan security** command.

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

Syntax Description

web-auth	Specifies web authentication.
enable	Enables the web authentication settings.
disable	Disables the web authentication settings.
acl	Configures an access control list.
server-precedence	Configures the authentication server precedence order for web authentication users.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
email-input	Configures the web captive portal using an e-mail address.
web-passthrough	Specifies the web captive portal with no authentication required.

Defaults

None.

Examples

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

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

Related Commands

[show remote-lan](#)

config remote-lan session-timeout

To configure client session timeout, use the **config remote-lan session-timeout** command.

config remote-lan session-timeout *remote-lan-id* *seconds*

Syntax Description	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
	<i>seconds</i>	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.
Defaults	None.	
Examples	This example shows how to configure the client session timeout to 6000 seconds for a remote LAN with ID 1: <pre>> config remote-lan session-timeout 1 6000</pre>	
Related Commands	show remote-lan	

config remote-lan webauth-exclude

To configure web authentication exclusion on a remote LAN, use the **config remote-lan webauth-exclude** command.

config remote-lan webauth-exclude *remote-lan-id* {enable | disable}

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
enable	Enables web authentication exclusion on the remote LAN.
disable	Disables web authentication exclusion on the remote LAN.

Defaults

None.

Examples

This example shows how to enable web authentication exclusion on a remote LAN with ID 1:

```
> config remote-lan webauth-exclude 1 enable
```

Related Commands

[show remote-lan](#)

Configure Memory Monitor Commands

To troubleshoot hard-to-solve or hard-to-reproduce memory problems, use the **config memory monitor** commands.

**Note**

The commands in this section can be disruptive to your system and should be run only when you are advised to do so by the Cisco Technical Assistance Center (TAC).

config memory monitor errors

To enable or disable monitoring for memory errors and leaks, use the **config memory monitor errors** command:

config memory monitor errors {enable | disable}



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

enable	Enables the monitoring for memory settings.
disable	Disables the monitoring for memory settings.

Defaults

Disabled by default.



Usage Guidelines

Note Be cautious about changing the defaults for the **config memory monitor** command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

Examples

This example shows how to enable monitoring for memory errors and leaks for a controller:

```
> config memory monitor errors enable
```

Related Commands

[config memory monitor leaks](#)
[debug memory](#)
[show memory monitor](#)

config memory monitor leaks

To configure the controller to perform an auto-leak analysis between two memory thresholds, use the **config memory monitor leaks** command.

config memory monitor leaks *low_thresh high_thresh*



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

<i>low_thresh</i>	Value below which free memory cannot fall without crashing. This value cannot be set lower than 10000 KB.
<i>high_thresh</i>	Value below which the controller enters auto-leak-analysis mode. See the “Usage Guidelines” section.

Defaults

The default value for *low_thresh* is 10000 KB; the default value for *high_thresh* is 30000 KB.



Usage Guidelines

Note Be cautious about changing the defaults for the **config memory monitor** command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

Use this command if you suspect that a memory leak has occurred.

If the free memory is lower than the *low_thresh* threshold, the system crashes, generating a crash file. The default value for this parameter is 10000 KB, and you cannot set it below this value.

Set the *high_thresh* threshold to the current free memory level or higher so that the system enters auto-leak-analysis mode. After the free memory reaches a level lower than the specified *high_thresh* threshold, the process of tracking and freeing memory allocation begins. As a result, the **debug memory events enable** command shows all allocations and frees, and the **show memory monitor detail** command starts to detect any suspected memory leaks.

Examples

This example shows how to set the threshold values for auto-leak-analysis mode to 12000 KB for the low threshold and 35000 KB for the high threshold:

```
> config memory monitor leaks 12000 35000
```

Related Commands

[config memory monitor errors](#)
[debug memory](#)
[show memory monitor](#)

Configure Mesh Commands

Use the **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

max-hop	Sets the maximum number of hops before triggering an alarm for traffic over the mesh network. The valid values are 1 to 16 (inclusive).
max-children	Sets the maximum number of mesh access points (MAPs) that can be assigned to a mesh router access point (RAP) before triggering an alarm. The valid values are 1 to 16 (inclusive).
low-snr	Sets the low-end signal-to-noise ratio (SNR) value before triggering an alarm. The valid values are 1 to 30 (inclusive).
high-snr	Sets the high-end SNR value before triggering an alarm. The valid values are 1 to 30 (inclusive).
association	Sets the mesh alarm association count value before triggering an alarm. The valid values are 1 to 30 (inclusive).
parent-change count	Sets the number of times a MAP can change its RAP association before triggering an alarm. The valid values are 1 to 30 (inclusive).
<i>value</i>	Triggers value above or below which an alarm is generated. The valid values vary for each command.

Defaults

See the “Syntax Description” section for command and argument value ranges.

Examples

This example shows how to set the maximum hops threshold to 8:

```
> config mesh alarm max-hop 8
```

This example shows how to set the upper SNR threshold to 25:

```
> 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](#)
[config mesh slot-bias](#)
[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

enable	Enables this feature for all outdoor mesh access points.
disable	Disables this feature for all outdoor mesh access points.

Defaults

None.

Examples

This example shows how to enable anti-stranding on all outdoor mesh access points:

```
> 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 backhaul rate-adapt

To globally configure the backhaul Tx rate adaptation (universal access) settings for indoor and outdoor mesh access points, use the **config mesh backhaul rate-adapt** command.

config mesh backhaul rate-adapt [**all** | **bronze** | **silver** | **gold** | **platinum**] {**enable** | **disable**}

Syntax Description

rate-adapt	Configures mesh backhaul Tx rate adaptation.
all	Grants <i>universal access</i> privileges on mesh access points.
bronze	Grants <i>background-level</i> client access privileges on mesh access points.
silver	Grants <i>best effort-level</i> client access privileges on mesh access points.
gold	Grants <i>video-level</i> client access privileges on mesh access points.
platinum	Grants <i>voice-level</i> client access privileges on mesh access points.
enable	Enables this backhaul access level for mesh access points.
disable	Disables this backhaul access level for mesh access points.

Defaults

Disabled.

Usage Guidelines

To use this command, mesh backhaul with client access must be enabled by using the [config mesh client-access](#) command.



Note After this feature is enabled, all mesh access points reboot.

Examples

This example shows how to set the backhaul client access to the best-effort level:

```
> config mesh backhaul rate-adapt silver
```

Related Commands

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

config mesh backhaul slot

To configure the slot radio as a downlink backhaul, use the **config mesh backhaul slot** command.

```
config mesh backhaul slot slot_id {enable | disable} cisco_ap
```

Syntax Description	<i>slot_id</i>	Slot number between 0 and 2.
	enable	Enables the entered slot radio as a downlink backhaul.
	disable	Disables the entered slot radio as a downlink backhaul.
	<i>cisco_ap</i>	Name of the Root AP of the sector on which the backhaul needs to be enabled or disabled.

Defaults	Disabled.

Usage Guidelines	For 2.4 GHz, only slot 0 and 1 are valid. If slot 0 is enabled, then slot 1 is automatically be disabled. If slot 0 is disabled, then slot 1 is automatically enabled. The config mesh backhaul slot command is applicable only to AP1522.

Examples	This example shows how to enable slot 1 as the preferred backhaul for the root AP myrootap1: <pre>> config mesh backhaul slot 1 enable myrootap1</pre>

Related Commands	show mesh ap show mesh config show mesh stats

config mesh battery-state

To configure the battery state for Cisco Aironet 1520 series mesh access points, use the **config mesh battery-state** command.

```
config mesh battery-state {enable | disable} {all | cisco_ap}
```

Syntax Description

enable	Enables the battery-state for 1520 series mesh access points.
disable	Disables the battery-state for 1520 series mesh access points.
all	Applies this command to all mesh access points.
cisco_ap	Specific mesh access point.

Defaults

Disabled.

Examples

This example shows how to set the backhaul client access to the best-effort level:

```
> 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 [extended] | disable}

Syntax Description

enable	Allows wireless client association over the mesh access point backhaul 802.11a radio.
disable	Restricts the 802.11a radio to backhaul traffic, and allows client association only over the 802.11b/g radio.
extended	Enables client access over both the backhaul radios for 1524 serial backhaul access points.

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, Cisco Aironet 1520 series (152x) mesh access points allow wireless client association over the 802.11a radio, which 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

This example shows how to enable client access extended to allow a wireless client association over the 802.11a radio:

```
> config mesh client-access enable extended
```

```
Enabling client access on both backhaul slots
Same BSSIDs will be used on both slots
All Mesh AP will be rebooted
Are you sure you want to start? (y/N) Y
```

This example shows how to restrict a wireless client association to the 802.11b/g radio:

```
> 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

[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	enable	Bridges packets as if they are untagged.
	disable	Drops all tagged packets.

Defaults Enabled.

Usage Guidelines 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 This example shows how to configure Ethernet packets as untagged:

```
> config mesh ethernet-bridging vlan-transparent enable
```

This example shows how to drop tagged Ethernet packets:

```
> 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

enable	Enables DFS for mesh access points.
disable	Disables DFS 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 a radar signal, the MAP will notify the root access point (RAP), and the RAP will initiate a sector change.

All MAPs and the RAP that belong to that sector go to a new channel, which 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, which means that if radar is frequently observed on a RAP's channel, it is important that you configure a different channel for that RAP to exclude the radar affected channel at the controller.

Examples

This example shows to enable full-sector DFS on mesh access points:

```
> config mesh full-sector-dfs enable
```

Related Commands

[config mesh alarm](#)
[config mesh battery-state](#)
[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

destination_ap_name 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 that you want link data from in the *dest_ap* argument. When the command completes, enter the **config mesh linkdata** command and list the same destination access point, to display 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.

MAC filtering 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

This example shows how to enable external MAC address filtering on access point AP001d.710d.e300:

```
> config mesh linkdata 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%

```

This example shows how to enable external MAC filtering on access point AP001d.71d.e300:

```
> 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	
<i>source_ap</i>	Source access point.
<i>dest_ap</i>	Destination access point.
<i>dest_MAC</i>	Destination MAC address.
<i>datarate</i>	- Data rate for 802.11a radios. Valid values are 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps. - Data rate for 802.11b radios. Valid values are 6, 12, 18, 24, 36, 54, or 100 Mbps. - Data rate for 802.11n radios. Valid values are MCS rates between m0 to m15.
<i>packet_rate</i>	Number of packets per second. Valid range is 1 through 3000, but the recommended default is 100.
<i>packet_size</i>	(Optional) Packet size in bytes. If not specified, packet size defaults to 1500 bytes.
<i>duration</i>	(Optional) 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 enter the **config mesh linktest** command with the access point that you want link data from in the *dest_ap* argument. When the command completes, enter the **config mesh linkdata** command and list the same destination access point, to display the link data.

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

This example shows how 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:

```
> 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%

```

Table 2-4 lists the output flags displayed for the **config mesh linktest** command.

Table 2-4 Output Flags for the Config Mesh Linktest Command

Output Flag	Description
txPkts	Number of packets sent by the source.
txBuffAllocErr	Number of linktest buffer allocation errors at the source (expected to be zero).
txQFullErrs	Number of linktest queue full errors at the source (expected to be zero).
Total rx pkts heard at destination	Number of linktest packets received at the destination (expected to be same as or close to the txPkts).
rx pkts decoded correctly	Number of linktest packets received and decoded correctly at the destination (expected to be same as close to txPkts).
err pkts: Total	Packet error statistics for linktest packets with errors.
rx lost packets	Total number of linktest packets not received at the destination.
rx dup pkts	Total number of duplicate linktest packets received at the destination.

Table 2-4 **Output Flags for the Config Mesh Linktest Command (continued)**

Output Flag	Description
rx out of order	Total number of linktest packets received out of order at the destination.
avgNF	Average noise floor.
Noise Floor profile	Noise floor profile in dB and are negative numbers.
avgSNR	Average SNR values.
SNR profile [odb...60dB]	Histogram samples received between 0 to 60 dB. The different columns in the SNR profile is the number of packets falling under the bucket 0-3, 3-6, 6-9, up to 57-60.
avgRSSI	Average RSSI values. The average high and low RSSI values are positive numbers.
RSSI profile [-100dB...-40dB]	The RSSI profile in dB and are negative numbers.

Related Commands

[config mesh battery-state](#)
[config mesh client-access](#)
[config mesh full-sector-dfs](#)
[config mesh linkdata](#)
[config mesh multicast](#)
[config mesh range](#)
[show mesh client-access](#)
[show mesh config](#)
[show mesh security-stats](#)
[show mesh stats](#)

config mesh lsc

To configure locally significant certificate (LSC) on mesh access points, use the **config mesh lsc** command.

config mesh lsc {enable | disable}

Syntax Description

enable	Enables LSC on mesh access points.
disable	Disables LSC on mesh access points.

Defaults

None.

Examples

This example shows how to enable LSC on mesh access points:

```
> config mesh lsc enable
```

Related Commands

[config certificate lsc](#)
[show certificate lsc](#)

config mesh multicast

To configure multicast mode settings to manage multicast transmissions within the mesh network, use the **config mesh multicast** command.

config mesh multicast {regular | in | in-out}

Syntax Description		
regular		Multicasts the video across the entire mesh network and all its segments by bridging-enabled root access points (RAPs) and mesh access points (MAPs).
in		Forwards the 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
in-out		Configures 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 Ethernet networks, 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 the Usage Guidelines section for more information.

Defaults

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 (by using the [config network multicast global](#) command). If multicast does not need to extend to 802.11b clients beyond the mesh network, you should disable the global multicast parameter.

Examples

This example shows how to multicast video across the entire mesh network and all its segments by bridging-enabled RAPs and MAPs:

```
> config mesh multicast regular
```

Related Commands

[config network multicast global](#)
[config mesh battery-state](#)
[config mesh client-access](#)
[config mesh linktest](#)
[show mesh ap](#)
[show mesh config](#)
[show mesh stats](#)

config mesh parent preferred

To configure a preferred parent for a mesh access point, use the **config mesh parent preferred** command.

```
config mesh parent preferred cisco_ap {mac_address | none}
```

Syntax Description

<i>cisco_ap</i>	Name of the child access point.
<i>mac_address</i>	MAC address of the preferred parent.
none	Clears the configured parent.

Defaults

None.

Usage Guidelines

A child AP selects the preferred parent based on the following conditions:

- The preferred parent is the best parent.
- The preferred parent has a link SNR of at least 20 dB (other parents, however good, are ignored).
- The preferred parent has a link SNR in the range of 12 dB and 20 dB, but no other parent is significantly better (that is, the SNR is more than 20 percent better). For an SNR lower than 12 dB, the configuration is ignored.
- The preferred parent is not blacklisted.
- The preferred parent is not in silent mode because of dynamic frequency selection (DFS).
- The preferred parent is in the same bridge group name (BGN). If the configured preferred parent is not in the same BGN and no other parent is available, the child joins the parent AP using the default BGN.

Examples

This example shows how to configure a preferred parent with the MAC address 00:21:1b:ea:36:60 for a mesh access point myap1:

```
> config mesh parent preferred myap1 00:21:1b:ea:36:60
```

This example shows how to clear a preferred parent with the MAC address 00:21:1b:ea:36:60 for a mesh access point myap1, by using the keyword **none**:

```
> config mesh parent preferred myap1 00:21:1b:ea:36:60 none
```

Related Commands

[config network multicast global](#)
[config mesh battery-state](#)
[config mesh client-access](#)
[config mesh linktest](#)
[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

enable	Enables the 4.9-GHz public safety band.
disable	Disables the 4.9-GHz public safety band.
all	Applies the command to all mesh access points.
<i>cisco_ap</i>	Specific mesh access point.

Defaults

Disabled.

Usage Guidelines

4.9 GHz is a licensed frequency band restricted to public-safety personnel.

Examples

This example shows how to enable the 4.9-GHz public safety band for all mesh access points:

```
> config 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

<i>index</i>	RADIUS authentication method. Options are as follows: - Enter eap to designate Extensible Authentication Protocol (EAP) for the mesh RADIUS server setting. - Enter psk to designate Preshared Keys (PSKs) for the mesh RADIUS server setting.
enable	Enables the external authentication for mesh access points.
disable	Disables the external authentication for mesh access points.

Defaults

EAP is enabled by default.

Examples

This example shows how to enable external authentication for mesh access points:

```
> 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	<i>distance</i>	(Optional) 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	This example shows how to set the range between an outdoor mesh RAP and a MAP:

```
> 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 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	
enable	Enables the secondary backhaul configuration.
force-same-secondary-channel	(Optional) 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 mesh access points (MAPs) at the second hop and beyond.
disable	Specifies the secondary backhaul configuration is disabled.
rll-transmit	Uses reliable link layer (RLL) at the second hop and beyond.
rll-retransmit	Extends the number of RLL retry attempts in an effort to improve reliability.

Defaults 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 This example shows how to enable a secondary backhaul radio and force all access points rooted at the first hop node to have the same secondary channel:

```
> config mesh secondary-backhaul enable force-same-secondary-channel
```

Related Commands

- [config mesh battery-state](#)
- [config mesh backhaul slot](#)
- [show mesh client-access](#)
- [show mesh config](#)
- [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

rad-mac-filter	Enables a RADIUS MAC address filter for the mesh security setting.
force-ext-auth	Disables forced external authentication for the mesh security setting.
enable	Enables the setting.
disable	Disables the setting.
eap	Designates the Extensible Authentication Protocol (EAP) for the mesh security setting.
psk	Designates preshared keys (PSKs) for the mesh security setting.

Defaults

EAP.

Examples

This example shows how to configure EAP as the security option for all mesh access points:

```
> config mesh security eap
```

This example shows how to configure PSK as the security option for all mesh access points:

```
> config mesh security psk
```

Related Commands

[config mesh alarm](#)
[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](#)

config mesh slot-bias

To enable or disable slot bias for serial backhaul mesh access points, use the **config mesh slot-bias** command.

config mesh slot-bias {enable | disable}

Syntax Description

enable	Enables slot bias for serial backhaul mesh APs.
disable	Disables slot bias for serial backhaul mesh APs.

Defaults

By default, slot bias is in enabled state.

Usage Guidelines

Follow these guidelines when using this command:

- The **config mesh slot-bias** command is a global command and therefore applicable to all 1524SB APs associated with the same controller.
- Slot bias is applicable only when both slot 1 and slot 2 are available. If a slot radio does not have a channel that is available because of dynamic frequency selection (DFS), the other slot takes up both the uplink and downlink roles.
- If slot 2 is not available because of hardware issues, slot bias functions normally. Corrective action should be taken by disabling the slot bias or fixing the antenna.

Examples

This example shows how to disable slot bias for serial backhaul mesh APs:

```
> config mesh slot-bias disable
```

Related Commands

[config mesh alarm](#)
[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

<i>username</i>	Account username. The username can be up to 24 alphanumeric characters.
<i>password</i>	Account password. The password can be up to 24 alphanumeric characters.
read-write	Creates a management user with read-write access.
read-only	Creates a management user with read-only access.
<i>description</i>	(Optional) Description of the account. The description can be up to 32 alphanumeric characters within double quotes.

Defaults

None.

Examples

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

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

Related Commands

show mgmtuser

config mgmtuser delete

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

config mgmtuser delete *username*

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

Defaults	None.

Examples	This example shows how to delete a management user account admin from the Cisco wireless LAN controller:

```
> config mgmtuser delete admin
```

```
Deleted user admin
```

Related Commands	show mgmtuser

config mgmtuser description

To add a description to an existing management user login to the Cisco wireless LAN controller, use the **config mgmtuser description** command.

config mgmtuser description *username description*

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

Defaults	None.

Examples	This example shows how to add a description “master-user” to the management user “admin”: <pre>> config mgmtuser description admin "master-user"</pre>

Related Commands	config mgmtuser add config mgmtuser delete config mgmtuser password show mgmtuser

config mgmtuser password

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

config mgmtuser password *username password*

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

Defaults	None.

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

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

Related Commands	show mgmtuser

Configure Mobility Commands

Use the **config mobility** commands to configure mobility (roaming) settings.

config mobility dscp

To configure the mobility intercontroller DSCP value, use the **config mobility dscp** command.

config mobility dscp *dscp_value*

Syntax Description

<i>dscp_value</i>	DSCP value ranging from 0 to 63.

Defaults

None.

Examples

This example shows how to configure the mobility intercontroller DSCP value to 40:

```
> config mobility dscp 40
```

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](#)

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

add	Adds or changes a mobility anchor to a wireless LAN.
delete	Deletes a mobility anchor from a wireless LAN.
wlan	Specifies the wireless LAN anchor settings.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512 (inclusive).
guest-lan	Specifies the 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

This example shows how to add a mobility anchor with the IP address 192.12.1.5 to a wireless LAN ID 2:

```
> config mobility group anchor add wlan 2 192.12.1.5
```

This example shows how to delete a mobility anchor with the IP address 193.13.1.15 from a wireless LAN:

```
> config mobility group anchor delete wlan 5 193.13.1.5
```

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	<i>domain_name</i> Domain name. The domain name can be up to 31 case-sensitive characters.

Defaults	None.

Examples	This example shows how to configure a mobility domain name lab1: <pre>> config mobility group domain lab1</pre>

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*

Syntax Description

<i>count</i>	Number of times that a ping request is sent to a mobility group member before the member is considered unreachable. The valid range is 3 to 20. The default is 3.

Defaults

3.

Examples

This example shows how to specify the number of times a ping request is sent to a mobility group member before the member is considered unreachable to 3 counts:

```
> 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** command.

config mobility group keepalive *interval*

Syntax Description	<i>interval</i>	Interval of time between each ping request sent to a mobility group member. The valid range is 1 to 30 seconds. The default value is 10 seconds.

Defaults	10 seconds.

Examples	This example shows how to specify the amount of time between each ping request sent to a mobility group member to 10 seconds:

```
> 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

add	Adds or changes a mobility group member to 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).
delete	(Optional) Deletes a mobility group member from the list.

Defaults

None.

Examples

This example shows how to add a mobility group member to the list:

```
> 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

To configure the multicast group IP address for nonlocal groups within the mobility list, use the **config mobility group multicast-address** command:

config mobility group multicast-address *group_name* *IP_address*

Syntax Description

<i>group_name</i>	Member switch group name (if different from the default group name).
<i>IP_address</i>	Member switch IP address.

Defaults

None.

Examples

This example shows how to configure the multicast group IP address 10.10.10.1 for a group named test:

```
> 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, use the **config mobility multicast-mode** command.

```
config mobility multicast-mode {enable | disable} local_group_multicast_address
```

Syntax Description	enable	Enables the multicast mode; the controller uses multicast mode to send Mobile Announce messages to the local group.
	disable	Disables the 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 This example shows how to enable the multicast mobility mode for the local mobility group IP address 157.168.20.0:

```
> 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

enable	Enables the mobility group message security.
disable	Disables mobility group message security.

Defaults

None.

Examples

This example shows how to enable the secure mode for mobility messages:

```
> 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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to reset the mobility group statistics:

> **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.

config msglog level critical

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Usage Guidelines	The message log always collects and displays critical messages, regardless of the message log level setting.

Examples	This example shows how to configure the message log severity level and display critical messages: <pre>> config msglog level critical</pre>

Related Commands	show msglog

config msglog level error

To reset the message log so that it collects and displays both critical (highest-level) and error (second-highest) messages, use the **config msglog level error** command.

config msglog level error

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to reset the message log to collect and display critical and noncritical error messages: <pre>> config msglog level error</pre>

Related Commands	show msglog

config msglog level security

To reset the message log so that it collects and displays critical (highest-level), error (second-highest), and security (third-highest) messages, use the **config msglog level security** command.

config msglog level security

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to reset the message log so that it collects and display critical, noncritical, and authentication or security-related errors:

> **config msglog level security**

Related Commands	show msglog

config msglog level verbose

To reset the message log so that it collects and displays all messages, use the **config msglog level verbose** command.

config msglog level verbose

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to reset the message logs so that it collects and display all messages: <pre>> config msglog level verbose</pre>

Related Commands	show msglog

config msglog level warning

To reset the message log so that it collects and displays critical (highest-level), error (second-highest), security (third-highest), and warning (fourth-highest) messages, use the **config msglog level warning** command.

config msglog level warning

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to reset the message log so that it collects and displays warning messages in addition to critical, noncritical, and authentication or security-related errors: <pre>> config msglog level warning</pre>

Related Commands	show msglog

Configure Media-Stream Commands

Use the **config media-stream** commands to configure media stream settings.

config 802.11 media-stream multicast-direct

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

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

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

Defaults None.

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

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

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

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

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

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

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

Related Commands

- [config 802.11 media-stream video-redirect](#)
- [show 802.11a media-stream name](#)
- [show media-stream group summary](#)
- [show media-stream group detail](#)

config 802.11 media-stream video-redirect

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

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

Syntax Description

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

Defaults

None.

Usage Guidelines

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

Examples

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

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

Related Commands

[config 802.11 media-stream multicast-direct](#)
[show 802.11a media-stream name](#)
[show media-stream group summary](#)
[show media-stream group detail](#)

config media-stream multicast direct

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

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

Syntax Description

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

Defaults

None.

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

show 802.11a media-stream name
 show media-stream group summary
 show media-stream group detail

config media-stream message

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

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

Syntax Description		
state		Specifies the media stream message state.
enable		Enables the session announcement message state.
disable		Disables the session announcement message state.
url		Configures the URL.
url		Session announcement URL.
email		Configures the email ID.
email		Specifies the session announcement e-mail.
phone		Configures the phone number.
phone_number		Session announcement phone number.
note		Configure the notes.
note		Session announcement notes.

Defaults	Disabled.

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

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

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

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

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

Related Commands	config media-stream show 802.11a media-stream name show media-stream group summary show media-stream group detail

config media-stream add

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

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

Syntax Description

multicast-direct	Specifies the media stream for the multicast-direct setting.
<i>media_stream_name</i>	Media-stream name.
<i>start-IP</i>	IP multicast destination start address.
<i>end-IP</i>	IP multicast destination end address
template	(Optional) Configures the media stream from templates.
very coarse	Applies a very-coarse template.
coarse	Applies a coarse template.
ordinary	Applies an ordinary template.
low-resolution	Applies a low-resolution template.
med-resolution	Applies a medium-resolution template.
high-resolution	Applies a high-resolution template.
detail	Configures the media stream with specific parameters.
<i>bandwidth</i>	Maximum expected stream bandwidth.
<i>packet-size</i>	Average packet size.
periodic	Specifies the periodic admission evaluation.
initial	Specifies the Initial admission evaluation.
<i>qos</i>	AIR QoS class (video only).
<i>priority</i>	Specifies the media-stream priority.
drop	Specifies that the stream is dropped on a periodic reevaluation.
fallback	Specifies if the stream is demoted to the best-effort class on a periodic reevaluation.

Defaults

None.

Usage Guidelines

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

Examples

This example shows how to configure a new media stream:

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

Related Commands

show 802.11a media-stream name

show media-stream group summary
show media-stream group detail

config media-stream admit

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

config media-stream admit *media_stream_name*

Syntax Description

<i>media_stream_name</i>	Media-stream group name.

Defaults

None.

Usage Guidelines

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

Examples

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

```
> config media-stream admit myMediaStream
```

Related Commands

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream deny

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

config media-stream block *media_stream_name*

Syntax Description	<i>media_stream_name</i> Media-stream group name.
Defaults	None.
Usage Guidelines	When you try to block traffic for the media stream group, you will be prompted that IGMP snooping will be disabled and enabled again, and all clients might observe a glitch on the multicast traffic.
Examples	This example shows how to block traffic for a media stream group: <pre>> config media-stream deny myMediaStream</pre>
Related Commands	show 802.11a media-stream name show media-stream group summary show media-stream group detail

config media-stream delete

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

config media-stream delete *media_stream_name*

Syntax Description

media_stream_name Media-stream name.

Defaults

None.

Usage Guidelines

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

Examples

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

```
> config media-stream delete abc
```

Related Commands

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

Configure Net User Commands

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

config netuser add

To add a guest user on a WLAN or wired guest LAN to the local user database on the controller, use the **config netuser add** command.

config netuser add *username password {wlan wlan_id | guestlan guestlan_id} userType guest lifetime lifetime description description*

Syntax Description

<i>username</i>	Guest username. The username can be up to 50 alphanumeric characters.
<i>password</i>	User password. The password can be up to 24 alphanumeric characters.
wlan	Specifies the wireless LAN identifier to associate with or zero for any wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier assigned to the user. A zero value associates the user with any wireless LAN.
guestlan	Specifies the guest LAN identifier to associate with or zero for any wireless LAN.
<i>guestlan_id</i>	Guest LAN ID
userType	Specifies the user type.
guest	Specifies the guest for the guest user.
lifetime	Specifies the lifetime.
<i>lifetime</i>	Lifetime value (60 to 259200 or 0) in seconds for the guest user. Note A value of 0 indicates an unlimited lifetime.
<i>description</i>	Short description of user. The description can be up to 32 characters enclosed in double-quotes.

Defaults

None.

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

show netuser

config netuser delete

config netuser delete

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

config netuser delete *username*

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

Defaults	None.

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

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

```
> config netuser delete able1
```

```
Deleted user able1
```

Related Commands	show netuser

config netuser description

To add a description to an existing net user, use the **config netuser description** command.

config netuser description *username description*

Syntax Description

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

Defaults

None.

Examples

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

```
> config netuser description able1 "HQ1 Contact"
```

Related Commands

show netuser

config netuser guest-role apply

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

config netuser guest-role apply *username role_name*

Syntax Description

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

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

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

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

Related Commands

config netuser guest-role create
config netuser guest-role delete

config netuser guest-role create

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

config netuser guest-role create *role_name*

Syntax Description

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

Defaults

None.

Usage Guidelines

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

Examples

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

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

Related Commands

config netuser guest-role delete

config netuser guest-role delete

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

config netuser guest-role delete *role_name*

Syntax Description

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

Defaults

None.

Examples

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

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

Related Commands

config netuser guest-role create

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

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

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

Syntax Description

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

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, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Examples

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

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

Related Commands

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

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

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

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

Syntax Description

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

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, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Examples

This example shows how to configure an average data rate for the QoS guest user named guestuser1 with the rate for TCP traffic of 0 Kbps:

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

Related Commands

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

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

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

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

Syntax Description

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

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, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Examples

This example shows how to configure the peak data rate for the QoS guest named guestuser1 with the rate for TCP traffic of 0 Kbps:

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

Related Commands

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

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

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

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

Syntax Description

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

Defaults

None.

Usage Guidelines

The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the quality of service (QoS) policy may block traffic to and from the wireless client.

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

Examples

This example shows how to configure a burst real-time rate for the QoS guest user named guestuser1 with the rate for TCP traffic of 0 Kbps:

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

Related Commands

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

config netuser maxEapUserLogin

To configure the maximum number of Extensible Authentication Protocol (EAP) user login attempts allowed for a network user, use the **config netuser maxEapUserLogin** command.

config netuser maxEapUserLogin *count*

Syntax Description	<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	This example shows how to configure the maximum number of EAP user login attempts to 8: <pre>> config netuser maxEapUserLogin 8</pre>	
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*

Syntax Description

<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

This example shows how to configure the maximum number of login sessions for a single user to 8:

```
> config netuser maxUserLogin 8
```

Related Commands

show netuser

config netuser password

To change a local network user password, use the **config netuser password** command.

config netuser password *username password*

Syntax Description	<i>username</i>	Network username. The username can be up to 24 alphanumeric characters.
	<i>password</i>	Network user password. The password can contain up to 24 alphanumeric characters.

Defaults	None.

Examples	This example shows how to change the network user password from aire1 to aire2: <pre>> config netuser password aire1 aire2</pre>

Related Commands	show netuser

config netuser wlan-id

To configure a wireless LAN ID for a network user, use the **config netuser wlan-id** command.

config netuser wlan-id *username wlan_id*

Syntax Description	<i>username</i>	Network username. The username can be 24 alphanumeric characters.
	<i>wlan_id</i>	Wireless LAN identifier to associate with the user. A zero value associates the user with any wireless LAN.

Defaults	None.

Examples	This example shows how to configure a wireless LAN ID 2 to associate with the user named aire1: <pre>> config netuser wlan-id aire1 2</pre>

Related Commands	show netuser show wlan summary

Configure Network Commands

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

config network 802.3-bridging

To enable or disable 802.3 bridging on a controller, use the **config network 802.3-bridging** command.

config network 802.3-bridging {enable | disable}

Syntax Description	enable	Enables the 802.3 bridging.
	disable	Disables the 802.3 bridging.

Defaults Disabled.

Usage Guidelines In controller software release 5.2, the software-based forwarding architecture for Cisco 2100 Series Controllers is being replaced with a new forwarding plane architecture. As a result, Cisco 2100 Series Controllers and the Cisco wireless LAN controller Network Module for Cisco Integrated Services Routers bridge 802.3 packets by default. Therefore, 802.3 bridging can now be disabled only on Cisco 4400 Series Controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch.

To determine the status of 802.3 bridging, enter the [show netuser guest-roles](#) command.

Examples This example shows how to enable the 802.3 bridging:

```
> config network 802.3-bridging enable
```

Related Commands [show netuser guest-roles](#)
[show network](#)

config network allow-old-bridge-aps

To configure an old bridge access point's ability to associate with a switch, use the **config network allow-old-bridge-aps** command.

config network allow-old-bridge-aps {enable | disable}

Syntax Description

enable	Enables the switch association.
disable	Disables the switch association.

Defaults

Enabled.

Examples

This example shows how to configure an old bridge access point to associate with the switch:

```
> config network allow-old-bridge-aps enable
```

Related Commands

show network summary

config network ap-discovery nat-ip-only

To configure the IP addresses that the controller sends in its CAPWAP discovery responses, use the **config network ap-discovery nat-ip-only** command.

config network ap-discovery nat-ip-only {enable | disable}

Syntax Description

enable	Enables the use of NAT IP only in discovery response.
disable	Enables use of both NAT IP and non-NAT IP in discovery response.

Defaults

Enabled.

Usage Guidelines

- If the **config interface nat-address management** command is set, then this command controls which address(es) are sent in the CAPWAP discovery responses.
- If all APs are on the outside of the NAT gateway of the controller, then enter the **config network ap-discovery nat-ip-only enable**, and only the management NAT address is sent.
- If the controller has both APs on the outside and the inside of its NAT gateway, then enter the **config network ap-discovery nat-ip-only disable** command, and both the management NAT address and the management inside address are sent. Ensure that you have entered the **config ap link-latency disable all** command to avoid stranding APs.

Related Commands

config interface nat-address management
config ap link-latency

config network ap-fallback

To configure Cisco lightweight access point fallback, use the **config network ap-fallback** command.

config network ap-fallback {enable | disable}

Syntax Description	enable	Enables the Cisco lightweight access point fallback.
	disable	Disables the Cisco lightweight access point fallback.

Defaults	Enabled.

Examples	This example shows how to enable the Cisco lightweight access point fallback: <pre>> config network ap-fallback enable</pre>

Related Commands	<code>show network summary</code>

config network ap-priority

To enable or disable the option to prioritize lightweight access points so that after a controller failure they reauthenticate by priority rather than on a first-come-until-full basis, use the **config network ap-priority** command.

config network ap-priority {enable | disable}

Syntax Description	enable	Enables the lightweight access point priority reauthentication.
	disable	Disables the lightweight access point priority reauthentication.

Defaults	Disabled.

Examples	This example shows how to enable the lightweight access point priority reauthorization: <pre>> config network ap-priority enable</pre>

Related Commands	config ap priority show ap summary show network summary

config network apple-talk

To configure AppleTalk bridging, use the **config network apple-talk** command.

config network apple-talk {enable | disable}

Syntax Description	enable	Enables the AppleTalk bridging.
	disable	Disables the AppleTalk bridging.

Defaults	None.

Examples	This example shows how to configure AppleTalk bridging: <pre>> config network apple-talk enable</pre>

Related Commands	show network summary

config network arptimeout

To set the Address Resolution Protocol (ARP) entry timeout value, use the **config network arptimeout** command.

config network arptimeout *seconds*

Syntax Description	<i>seconds</i>	Timeout in seconds. The minimum value is 10. The default value is 300.
Defaults	300.	
Examples	This example shows how to set the ARP entry timeout value to 240 seconds: > config network arptimeout 240	
Related Commands	show network summary	

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

config network bridging-shared-secret *shared_secret*

Syntax Description

<i>shared_secret</i>	Bridging shared secret string. The string can contain up to 10 bytes.

Defaults

Enabled.

Usage Guidelines

This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.

The zero-touch configuration must be enabled for this command to work.

Examples

This example shows how to configure the bridging shared secret string “shhh1”:

```
> config network bridging-shared-secret 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

enable	Enables the broadcast packet forwarding.
disable	Disables the broadcast packet forwarding.

Defaults

Disabled.

Usage Guidelines

This command allows you to enable or disable broadcasting. You must enable multicast mode before enabling broadcast forwarding. Use the **config network multicast mode command** to configure multicast mode on the controller.



Note

The default multicast mode is unicast in case of all controllers except for Cisco 2106 Controllers.

The broadcast packets and multicast packets can be independently controlled. If multicast is off and broadcast is on, broadcast packets still reach the access points, based on the configured multicast mode.

Examples

This example shows how to enable broadcast packet forwarding:

```
> config network broadcast enable
```

Related Commands

```
show network summary  
config network multicast global  
config network multicast mode
```

config network fast-ssid-change

To enable or disable fast Service Set Identifier (SSID) changing for mobile stations, use the **config network fast-ssid-change** command.

config network fast-ssid-change {enable | disable}

Syntax Description

enable	Enables the fast SSID changing for mobile stations
disable	Disables the fast SSID changing for mobile stations.

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

This example shows how to enable the fast SSID changing for mobile stations:

```
> config network fast-ssid-change enable
```

Related Commands

show network summary

config network ip-mac-binding

To validate the source IP address and MAC address binding within client packets, use the **config network ip-mac-binding** command.

config network ip-network-binding {enable | disable}

Syntax Description

enable	Enables this command.
disable	Disables this command.

Command Default

Enabled.

Usage Guidelines

In controller software release 5.2, the controller enforces strict IP address-to-MAC address binding in client packets. The controller checks the IP address and MAC address in a packet, compares them to the addresses that are registered with the controller, and forwards the packet only if they both match. In previous releases, the controller checks only the MAC address of the client and ignores the IP address.



Note

You might want to disable this binding check if you have a routed network behind a workgroup bridge (WGB).

Examples

This example shows how to validate the source IP and MAC address within client packets:

```
> config network ip-network-binding enable
```

config network master-base

To enable or disable the Cisco wireless LAN controller as an access point default master, use the **config network master-base** command.

config network master-base {enable | disable}

Syntax Description

enable	Enables the Cisco wireless LAN controller acting as a Cisco lightweight access point default master.
disable	Disables the Cisco wireless LAN controller acting as a Cisco lightweight access point default master.

Defaults

None.

Usage Guidelines

This setting is only used upon network installation and should be disabled after the initial network configuration. Because the Master Cisco wireless LAN controller is normally not used in a deployed network, the Master Cisco wireless LAN controller setting can be saved from 6.0.199.0 or later releases.

Examples

This example shows how to enable the Cisco wireless LAN controller as a default master:

```
> config network master-base enable
```

config network mgmt-via-wireless

To enable Cisco wireless LAN controller management from an associated wireless client, use the **config network mgmt-via-wireless** command.

config network mgmt-via-wireless {enable | disable}

Syntax Description

enable	Enables the switch management from a wireless interface.
disable	Disables the switch management from a wireless interface.

Defaults

Disabled.

Usage Guidelines

This feature allows wireless clients to manage only the Cisco wireless LAN controller associated with the client and the associated Cisco lightweight access point. That is, clients cannot manage another Cisco wireless LAN controller with which they are not associated.

Examples

This example shows how to configure switch management from a wireless interface:

```
> config network mgmt-via-wireless enable
```

Related Commands

show network summary

config network multicast global

To enable or disable multicasting on the controller, use the **config network multicast global** command.

```
config network multicast global {enable | disable}
```

Syntax Description	enable	Enables the multicast global support.
	disable	Disables the multicast global support.

Defaults	Disabled.

Usage Guidelines	The config network broadcast {enable disable} command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. This command uses the multicast mode configured on the controller (by using the config network multicast mode command) to operate.

Examples	This example shows how to enable the global multicast support: > config network multicast global enable

Related Commands	show network summary config network broadcast config network multicast mode

config network multicast igmp query interval

To configure the IGMP query interval, use the **config network multicast igmp query interval** command.

config network multicast igmp query interval *value*

Syntax Description	<i>value</i>	Frequency at which controller sends IGMP query messages. The range is from 15 to 2400 seconds.

Defaults	20 seconds.

Usage Guidelines	To configure IGMP query interval, ensure that you do the following: • Enable the global multicast by entering the config network multicast global enable command. • Enable IGMP snooping by entering the config network multicast igmp snooping enable command.

Examples	This example shows how to configure the IGMP query interval at 20 seconds: <pre>> config network multicast igmp query interval 20</pre>

Related Commands	config network multicast global config network multicast igmp snooping config network multicast igmp timeout

config network multicast igmp snooping

To enable or disable IGMP snooping, use the **config network multicast igmp snooping** command.

```
config network multicast igmp snooping {enable | disable}
```

Syntax Description	enable	Enables IGMP snooping.
	disable	Disables IGMP snooping.

Defaults	None.

Examples	This example shows how to enable internet IGMP snooping settings: > config network multicast igmp snooping enable

Related Commands	config network multicast global config network multicast igmp query interval config network multicast igmp timeout

config network multicast igmp timeout

To set the IGMP timeout value, use the **config network multicast igmp timeout** command.

config network multicast igmp timeout *value*

Syntax Description	<i>value</i> Timeout range from 30 to 7200 seconds.
Defaults	None.
Usage Guidelines	You can enter a timeout value between 30 and 7200 seconds. The controller sends three queries in one timeout value at an interval of <i>timeout</i> /3 to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.
Examples	This example shows how to configure the timeout value 50 for IGMP network settings: > config network multicast igmp timeout 50
Related Commands	config network multicast global config network multicast igmp snooping config network multicast igmp query interval

config network multicast mode multicast

To configure the controller to use the multicast method to send broadcast or multicast packets to an access point, use the **config network multicast mode multicast** command.

config network multicast mode multicast

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to configure the multicast mode to send a single copy of data to multiple receivers:

```
> config network multicast mode multicast
```

Related Commands	config network multicast global config network broadcast config network multicast mode unicast

config network multicast mode unicast

To configure the controller to use the unicast method to send broadcast or multicast packets to an access point, use the **config network multicast mode unicast** command.

config network multicast mode unicast

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to configure the controller to use the unicast mode: <pre>> config network multicast mode unicast</pre>

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

enable	Enables the OTAP provisioning.
disable	Disables the OTAP provisioning.

Defaults

Enabled.

Examples

This example shows how to disable the OTAP provisioning:

```
> config network otap-mode disable
```

Related Commands

show network summary

config network rf-network-name

To set the RF-Network name, use the **config network rf-network-name** command.

config network rf-network-name *name*

Syntax Description	<i>name</i> RF-Network name. The name can contain up to 19 characters.
Defaults	None.
Examples	This example shows how to set the RF-network name to travelers: <pre>> config network rf-network-name travelers</pre>
Related Commands	show network summary

config network secureweb

To change the state of the secure web (https is http and SSL) interface, use the **config network secureweb** command.

config network secureweb {enable | disable}

Syntax Description

enable	Enables the secure web interface.
disable	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

This example shows how to enable the secure web interface settings:

```
> config network secureweb enable
```

You must reboot for the change to take effect.

Related Commands

[config network secureweb cipher-option](#)
[show network summary](#)

config network secureweb cipher-option

To enable or disable secure web mode with increased security, or to enable or disable Secure Sockets Layer (SSL v2) for web administration and web authentication, use the **config network secureweb cipher-option** command.

config network secureweb cipher-option {high | sslv2} {enable | disable}

Syntax Description	high	Configures whether or not 128-bit ciphers are required for web administration and web authentication.
	sslv2	Configures SSLv2 for both web administration and web authentication.
	enable	Enables the secure web interface.
	disable	Disables the secure web interface.

Defaults The default is disabled for secure web mode with increased security and **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 This example shows how to enable secure web mode with increased security:

```
> config network secureweb cipher-option high enable
```

This example shows how to disable SSL v2:

```
> config network secureweb cipher-option sslv2 disable
```

Related Commands [config network secureweb](#)
[show network summary](#)

config network ssh

To allow or disallow new Secure Shell (SSH) sessions, use the **config network ssh** command.

config network ssh {enable | disable}

Syntax Description

enable	Allows the new SSH sessions.
disable	Disallows the new SSH sessions.

Defaults

Disabled.

Examples

This example shows how to enable the new SSH session:

```
> config network ssh enable
```

Related Commands

show network summary

config network telnet

To allow or disallow new Telnet sessions, use the **config network telnet** command.

config network telnet {enable | disable}

Syntax Description	enable	Allows new Telnet sessions.
	disable	Disallows new Telnet sessions.

Defaults	Disabled.

Examples	This example shows how to configure the new Telnet sessions: <pre>> config network telnet enable</pre>

Related Commands	config ap telnet show network summary

config network usertimeout

To change the timeout for idle client sessions, use the **config network usertimeout** command.

config network usertimeout *seconds*

Syntax Description	<i>seconds</i>	Recommended user idle timeout in seconds between 90 and 100000. The valid range is 15 to 100000 seconds. The default value is 300 seconds.
Defaults	300 seconds.	
Examples	This example shows how to configure the idle session timeout to 1200 seconds: > config network usertimeout 1200	
Related Commands	show network summary	

config network web-auth-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

<i>port</i>	Port number. The valid range is from 0 to 65535.

Defaults

None.

Examples

This example shows how to configure an additional port number 1200 to be redirected for web authentication:

```
> config network web-auth port 1200
```

Related Commands

show network summary

config network webmode

To enable or disable the web mode, use the **config network webmode** command.

```
config network webmode {enable | disable}
```

Syntax Description	enable	Enables the web interface.
	disable	Disables the web interface.

Defaults Enabled.

Examples This example shows how to disable the web interface mode:
> config network webmode disable

Related Commands show network summary

config network web-auth

To configure the network-level web authentication options, use the **config network web-auth** command.

config network web-auth {**port** *port-number*} | {**proxy-redirect** {**enable** | **disable**}}

Syntax Description	port	Configures additional ports for web authentication redirection.
	<i>port-number</i>	Port number (between 0 and 65535).
	proxy-redirect	Configures proxy redirect support for web authentication clients.
	enable	Enables proxy redirect support for web authentication clients.
	disable	Disables proxy redirect support for web authentication clients.

Note Web-auth Proxy redirection will be enabled for ports 80, 8080, and 3128, along with user defined port 345.

Defaults Disabled.

Usage Guidelines You must reset the system for the configuration to take effect.

Examples This example shows how to enable proxy redirect support for web authentication clients:

```
> config network web-auth proxy-redirect enable
```

Related Commands

- show network summary
- show run-config

config network zero-config

To configure bridge access point ZeroConfig support, use the **config network zero-config** command.

config network zero-config {enable | disable}

Syntax Description

enable	Enables the bridge access point ZeroConfig support.
disable	Disables the bridge access point ZeroConfig support.

Defaults

Enabled.

Examples

This example shows how to enable the bridge access point ZeroConfig support:

```
> config network zero-config enable
```

Related Commands

show network summary

config nmsp notify-interval measurement

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **config nmsp notify-interval measurement** command.

config nmsp notify-interval measurement { **client** | **rfid** | **rogue** } *interval*

Syntax Description

client	Modifies the interval for clients.
rfid	Modifies the interval for active radio frequency identification (RFID) tags.
rogue	Modifies the interval for rogue access points and rogue clients.
<i>interval</i>	Time interval. The range is from 1 to 30 seconds.

Defaults

None.

Usage Guidelines

The TCP port (16113) that the controller and location appliance communicate over must be open (not blocked) on any firewall that exists between the controller and the location appliance for NMSP to function.

Examples

This example shows how to modify the NMSP notification interval for the active RFID tags to 25 seconds:

```
> config nmsp notify-interval measurement rfid 25
```

Related Commands

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

config paging

To enable or disable scrolling of the page, use the **config paging** command.

config paging {enable | disable}

Syntax Description

enable	Enables the scrolling of the page.
disable	Disables the scrolling of the page.

Defaults

Enabled.

Related Commands

[show run-config](#)

config passwd-cleartext

To enable or disable temporary display of passwords in plain text, use the **config passwd-cleartext** command.

config passwd-cleartext {enable | disable}

Syntax Description

enable	Enables the display of passwords in plain text.
disable	Disables the display of passwords in plain text.

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

This example shows how to enable display of passwords in plain text:

```
> config passwd-cleartext enable
```

```
The way you see your passwds will be changed  
You are being warned.
```

```
Enter admin password:
```

Related Commands

[show run-config](#)

config pmk-cache delete

To delete an entry in the Pairwise Master Key (PMK) cache from all Cisco wireless LAN controllers in the mobility group, use the **config pmk-cache delete** command.

config pmk-cache delete {all | *mac_address*}

Syntax Description

all	Deletes all Cisco wireless LAN controllers.
<i>mac_address</i>	MAC address of the Cisco wireless LAN controller to delete.

Defaults

None.

Examples

This example shows how to delete all entries in the PMK cache:

```
> 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

all	Configures all ports.
<i>port</i>	Number of the port.
enable	Enables the specified ports.
disable	Disables the specified ports.

Defaults

Enabled.

Examples

This example shows how to disable port 8:

```
> config port adminmode 8 disable
```

This example shows how 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

all	Configures all ports.
<i>port</i>	Number of the port.
enable	Enables the specified ports.
disable	Disables the specified ports.

Defaults

The default for all ports is that autonegotiation is enabled.

Usage Guidelines

You must disable port autoconfiguration before you make physical mode manual settings by using the **config port physicalmode** command. The **config port autoneg** command overrides settings that you made using the **config port physicalmode** command.

Examples

This example shows how to turn on physical port autonegotiation for all front-panel Ethernet ports:

```
> config port autoneg all enable
```

This example shows how 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

all	Configures all ports.
<i>port</i>	Number of the port.
enable	Enables the specified ports.
disable	Disables the specified ports.

Defaults

Enabled.

Examples

This example shows how to disable port 8 traps:

```
> config port linktrap 8 disable
```

This example shows how 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

all	Configures all ports.
<i>port</i>	Number of the port.
enable	Enables the specified ports.
disable	Disables the specified ports.

Defaults

Enabled.

Examples

This example shows how to enable multicast appliance service on all ports:

```
> config port multicast appliance all enable
```

This example shows how to disable multicast appliance service on port 8:

```
> 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-duplex or full-duplex operation, use the **config port physicalmode** command.

config port physicalmode {**all** | *port*} {**100h** | **100f** | **10h** | **10f**}

Syntax Description

all	Configures all ports.
<i>port</i>	Number of the port.
100h	Specifies 100-Mbps/half-duplex operation.
100f	Specifies 100-Mbps/full-duplex operation.
10h	Specifies 10-Mbps/half-duplex operation.
10f	Specifies 10-Mbps/full-duplex operation.

Defaults

The default is that all ports are set to autonegotiate.

Usage Guidelines

You must disable autonegotiation by using the **config port autoneg** command before manually configuring any port's physical mode. The **config port autoneg** command overrides settings that you made using the **config port physicalmode** command.

Examples

This example shows how to set all ports to 100-Mbps/full-duplex operation:

```
> config port physicalmode all 100f
```

This example shows how to set port 20 to 100-Mbps/half-duplex operation:

```
> config port physicalmode 20 100h
```

This example shows how to set port 21 to 10-Mbps/full-duplex operation:

```
> config port physicalmode 21 10f
```

This example shows how 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

all	Configures all ports.
<i>port</i>	Port number.
enable	Enables the specified ports.
disable	Disable the specified ports.

Defaults

Enabled.

Examples

This example shows how to enable PoE on all ports:

```
> config port power all enable
```

This example shows how to disable PoE on port 8:

```
> config port power 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*

Syntax Description

<i>prompt</i>	New CLI system prompt enclosed in double quotes. The prompt can be up to 31 alphanumeric characters and is case sensitive.

Defaults

The system prompt is configured using the startup wizard.

Usage Guidelines

Because the system prompt is a user-defined variable, it is omitted from the rest of this documentation.

Examples

This example shows how to change the CLI system prompt to Cisco 4400:

```
> config prompt "Cisco 4400"
```

config 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

bronze	Specifies the average data rate for the queue bronze.
silver	Specifies the average data rate for the queue silver.
gold	Specifies the average data rate for the queue gold.
platinum	Specifies the average data rate for the queue platinum.
rate	Average data rate for TCP traffic per user. A value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Defaults

None.

Examples

This example shows how to configure the average data rate 0 Kbps for the queue gold:

```
> 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	bronze	Specifies the average real-time data rate for the queue bronze.
	silver	Specifies the average real-time data rate for the queue silver.
	gold	Specifies the average real-time data rate for the queue gold.
	platinum	Specifies the average real-time data rate for the queue platinum.
	<i>rate</i>	Average real-time data rate for TCP traffic per user. A value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Defaults None.

Examples This example shows how to configure the average real-time actual rate for queue gold:

```
> config qos average-realtime-rate gold 10
```

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	bronze	Specifies the peak data rate for the queue bronze.
	silver	Specifies the peak data rate for the queue silver.
	gold	Specifies the peak data rate for the queue gold.
	platinum	Specifies the peak data rate for the queue platinum.
	rate	Peak data rate for TCP traffic per user. A value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Defaults None.

Examples This example shows how to configure the peak rate 30000 Kbps for the queue gold:

```
> config qos burst-data-rate gold 30000
```

Related Commands

- show qos description
- config 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 burst 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

bronze	Specifies the burst real-time data rate for the queue bronze.
silver	Specifies the burst real-time data rate for the queue silver.
gold	Specifies the burst real-time data rate for the queue gold.
platinum	Specifies the burst real-time data rate for the queue platinum.
rate	Burst real-time data rate for TCP traffic per user. A value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Defaults

None.

Examples

This example shows how to configure the burst real-time actual rate 2000 Kbps for the queue gold:

```
> config qos burst-realtime-rate gold 2000
```

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	bronze	Specifies the QoS profile description for the queue bronze.
	silver	Specifies the QoS profile description for the queue silver.
	gold	Specifies the QoS profile description for the queue gold.
	platinum	Specifies the QoS profile description for the queue platinum.
	<i>description</i>	QoS profile description.

Defaults	None.

Examples	This example shows how to configure the QoS profile description “description” for the queue gold: <pre>> config qos description gold abc</pre>

Related Commands	show qos average-data-rate config qos burst-data-rate config qos average-realtime-rate config qos burst-realtime-rate config qos max-rf-usage

config qos max-rf-usage

To specify the maximum percentage of RF usage per access point, use the **config qos max-rf-usage** command.

config qos max-rf-usage {bronze | silver | gold | platinum} usage_percentage

Syntax Description

bronze	Specifies the maximum percentage of RF usage for the queue bronze.
silver	Specifies the maximum percentage of RF usage for the queue silver.
gold	Specifies the maximum percentage of RF usage for the queue gold.
platinum	Specifies the maximum percentage of RF usage for the queue platinum.
<i>usage_percentage</i>	Maximum percentage of RF usage.

Defaults

None.

Examples

This example shows how to specify the maximum percentage of RF usage for the queue gold:

```
> config qos max-rf-usage gold 20
```

Related Commands

show qos description
config qos average-data-rate
config qos burst-data-rate
config qos average-realtime-rate
config qos burst-realtime-rate

config qos dot1p-tag

To define the maximum value (0-7) for the priority tag associated with packets that fall within the profile, use the **config qos dot1p-tag** command.

config qos dot1p-tag {bronze | silver | gold | platinum} dot1p_tag

Syntax Description

bronze	Specifies the QoS 802.1p tag for the queue bronze.
silver	Specifies the QoS 802.1p tag for the queue silver.
gold	Specifies the QoS 802.1p tag for the queue gold.
platinum	Specifies the QoS 802.1p tag for the queue platinum.
<i>dot1p_tag</i>	Dot1p tag value between 1 and 7.

Defaults

None.

Examples

This example shows how to configure the a QoS 802.1p tag for the queue gold with the dot1p tag value of 5:

```
> config qos dot1p-tag gold 5
```

Related Commands

show qos queue_length all
config qos protocol-type

config qos protocol-type

To define the maximum value (0-7) for the priority tag associated with packets that fall within the profile, use the **config qos protocol-type** command.

config qos protocol-type {bronze | silver | gold | platinum} {none | dot1p}

Syntax Description

bronze	Specifies the QoS 802.1p tag for the queue bronze.
silver	Specifies the QoS 802.1p tag for the queue silver.
gold	Specifies the QoS 802.1p tag for the queue gold.
platinum	Specifies the QoS 802.1p tag for the queue platinum.
none	Specifies when no specific protocol is assigned.
<i>dot1p</i>	Specifies when dot1p type protocol is assigned.

Defaults

None.

Examples

This example shows how to configure the QoS protocol type silver:

```
> config qos protocol-type silver dot1p
```

Related Commands

show qos queue_length all
config qos dot1p-tag

config qos queue_length

To specify the maximum number of packets that access points keep in their queues, use the **config qos queue_length** command.

config qos queue_length {bronze | silver | gold | platinum} queue_length

Syntax Description	bronze	Specifies the QoS length for the queue bronze.
	silver	Specifies the QoS length for the queue silver.
	gold	Specifies the QoS length for the queue gold.
	platinum	Specifies the QoS length for the queue platinum.
	<i>queue_length</i>	Maximum queue length values (10 to 255).

Defaults	None.

Examples	This example shows how to configure the QoS length for the queue “gold” with the maximum queue length value as 12:

```
> config qos queue_length gold 12
```

Related Commands	show qos

Configure 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
enable	Enables a RADIUS accounting server.
disable	Disables a RADIUS accounting server.
delete	Deletes a RADIUS accounting server.
<i>index</i>	RADIUS server index. The controller begins the search with 1.
add	Adds a RADIUS accounting server.
<i>index_server_ip</i>	IP address of RADIUS server.
<i>port</i>	RADIUS server's UDP port number for the interface protocols.
ascii	Specifies the RADIUS server's secret type: ascii .
hex	Specifies the RADIUS server's secret type: hex .
<i>secret</i>	RADIUS server's secret.

Defaults

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

Examples

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

```
> config radius acct add 1 10.10.10.10 1813 ascii admin
```

Related Commands

[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	hmac-md5	Enables IPsec HMAC-MD5 authentication.
	hmac-sha1	Enables IPsec HMAC-SHA1 authentication.
	<i>index</i>	RADIUS server index.

Defaults	None.

Examples	This example shows how to configure the IPsec hmac-md5 authentication service on the RADIUS accounting server index 1:

```
> 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	<i>index</i> RADIUS server index.
Defaults	None.
Examples	This example shows how to disable the IPsec support for RADIUS accounting server index 1: > 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

<i>index</i>	RADIUS server index.

Defaults

None.

Examples

This example shows how to enable the IPsec support for RADIUS accounting server index 1:

```
> 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	3des	Enables IPsec 3DES encryption.
	aes	Enables IPsec AES encryption.
	des	Enables IPsec DES encryption.
	<i>index</i>	RADIUS server index value of between 1 and 17.

Defaults None.

Examples This example shows how to configure the IPsec 3DES encryption for RADIUS server index value 3:

```
> 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	IPsec	Configures the IPsec.
	ike	Configures the IKE.
	dh-group	Specifies the Dixie-Hellman group.
	group-1	Configures the DH Group 1 (768 bits).
	group-2	Configures the DH Group 2 (1024 bits).
	group-5	Configures the DH Group 5 (1024 bits).
	lifetime	Configures the IKE lifetime.
	<i>seconds</i>	IKE lifetime in seconds.
	phase1	Configures the IKE phase1 node.
	aggressive	Enables the aggressive mode.
	main	Enables the main mode.
	<i>index</i>	RADIUS server index.

Defaults None.

Examples This example shows how to configure an IKE lifetime of 23 seconds for RADIUS server index 1:

```
> 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

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

Defaults

The default delimiter is a hyphen.

Examples

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

```
> 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	<i>index</i>	RADIUS server index.
	enable	Enables the server as a network user's default RADIUS server.
	disable	Disables the server as a network user's default RADIUS server.

Defaults	None.

Examples	This example shows how to configure a default RADIUS accounting server for the network users with RADIUS server index1: <pre>> config radius acct network 1 enable</pre>

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	<i>index</i>	RADIUS server index.
	<i>timeout</i>	Number of seconds (from 2 to 30) between retransmissions.

Defaults	None.

Examples	This example shows how to configure retransmission timeout value 5 seconds between the retransmission: <pre>> config radius acct retransmit-timeout 5</pre>

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
enable	Enables a RADIUS authentication server.
disable	Disables a RADIUS authentication server.
delete	Deletes a RADIUS authentication server.
<i>index</i>	RADIUS server index. The controller begins the search with 1.
add	Adds a RADIUS authentication server. See the “Defaults” section.
<i>server_ip</i>	IP address of the RADIUS server.
<i>port</i>	RADIUS server’s UDP port number for the interface protocols.
ascii	Specifies RADIUS server’s secret type: ascii .
hex	Specifies RADIUS server’s secret type: hex .
<i>secret</i>	RADIUS server’s secret.

Defaults

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

Examples

This example shows how to configure a priority 1 RADIUS authentication server at 10.10.10.10 using port 1812 with a login password of *admin*:

```
> 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

hmac-md5	Enables IPsec HMAC-MD5 authentication.
hmac-sha1	Enables IPsec HMAC-SHA1 authentication.
<i>index</i>	RADIUS server index.

Defaults

None.

Examples

This example shows how to configure the IPsec hmac-md5 support for RADIUS authentication server index 1:

```
> 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

enable	Enables the IPsec support for an authentication server.
disable	Disables the IPsec support for an authentication server.
<i>index</i>	RADIUS server index.

Defaults

None.

Examples

This example shows how to enable the IPsec support for RADIUS authentication server index 1:

```
> config radius auth IPsec enable 1
```

This example shows how to disable the IPsec support for RADIUS authentication server index 1:

```
> config radius auth IPsec disable 1
```

Related Commands

show radius acct statistics

config radius auth IPsec encryption

To configure IPsec encryption 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

3des	Enables the IPsec 3DES encryption.
aes	Enables the IPsec AES encryption.
des	Enables the IPsec DES encryption.
index	RADIUS server index.

Defaults

None.

Examples

This example shows how to configure IPsec 3des encryption RADIUS authentication server index 3:

```
> config radius auth IPsec encryption 3des 3
```

Related Commands

show radius acct statistics

config radius auth IPsec ike

To configure Internet Key Exchange (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		
dh-group		Configures the IKE Diffie-Hellman group.
group-1		Configures the DH Group 1 (768 bits).
group-2		Configures the DH Group 2 (1024 bits).
group-5		Configures the DH Group 2 (1024 bits).
lifetime		Configures the IKE lifetime.
<i>seconds</i>		Lifetime in seconds.
phase1		Configures the IKE phase1 mode.
aggressive		Enables the aggressive mode.
main		Enables the main mode.
<i>index</i>		RADIUS server index.

Defaults	None.

Examples	This example shows how to configure IKE lifetime of 23 seconds for RADIUS authentication server index 1:

```
> config radius auth IPsec ike lifetime 23 1
```

Related Commands	show radius acct statistics

config radius auth keywrap

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

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

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

Defaults	None.

Examples	This example shows how to enable the AES key wrap for a RADIUS authentication server: <pre>> config radius auth keywrap enable</pre>

Related Commands	<code>show radius auth statistics</code>

config radius auth mac-delimiter

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

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

Syntax Description

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

Defaults

The default delimiter is a hyphen.

Examples

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

```
> 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	<i>index</i>	RADIUS server index.
	enable	Enables the server as a management user’s default RADIUS server.
	disable	Disables the server as a management user’s default RADIUS server.

Defaults None.

Examples This example shows how to configure a RADIUS server for management users:
> 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	<i>index</i>	RADIUS server index.
	enable	Enables the server as a network user default RADIUS server.
	disable	Disables the server as a network user default RADIUS server.

Defaults

None.

Examples

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

```
> config radius auth network 1 enable
```

Related Commands

show radius acct statistics

config radius acct network

config radius auth retransmit-timeout

To change a default transmission timeout for a RADIUS authentication server for the Cisco wireless LAN controller, use the **config radius auth retransmit-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description

<i>index</i>	RADIUS server index.
<i>timeout</i>	Number of seconds (from 2 to 30) between retransmissions.

Defaults

None.

Examples

This example shows how to configure a retransmission timeout of 5 seconds for a RADIUS authentication server:

```
> config radius auth retransmit-timeout 5
```

Related Commands

show radius auth statistics

config radius auth rfc3576

To configure RADIUS RFC-3576 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

enable	Enables RFC-3576 support for an authentication server.
disable	Disables RFC-3576 support for an authentication server.
<i>index</i>	RADIUS server index.

Defaults

None.

Usage Guidelines

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

Examples

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

```
> config radius auth rfc3576 enable 2
```

Related Commands

show radius auth statistics
show radius summary
show radius rfc3576

config radius auth server-timeout

To configure a retransmission timeout value for a RADIUS accounting server, use the **config radius auth server-timeout** command.

config radius auth server-timeout *index timeout*

Syntax Description	<i>index</i>	RADIUS server index.
	<i>timeout</i>	Timeout value. The range is 2 to 30 seconds.

Defaults The default timeout is 2 seconds.

Examples This example shows how to configure a server timeout value of 2 seconds for RADIUS authentication server index 10:

```
> config radius auth server-timeout 2 10
```

Related Commands

- show radius auth statistics
- show radius summary

config radius aggressive-failover disabled

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

config radius aggressive-failover disabled

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to configure the controller to mark a RADIUS server as down: > config radius aggressive-failover disabled

Related Commands	show radius summary

config radius backward compatibility

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

config radius backward compatibility {enable | disable}

Syntax Description

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

Defaults

Enabled.

Examples

This example shows how to enable the RADIUS backward compatibility settings:

```
> 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.

config radius callStationIdType {ipAddr | macAddr | ap-macAddr}

Syntax Description	ipAddr	Configures the Call Station ID type to use the IP address (only Layer 3).
	macAddr	Configures the Call Station ID type to use the system's MAC address (Layers 2 and 3).
	ap-macAddr	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3).
Defaults	Enabled.	
Usage Guidelines	This command uses the selected calling station ID for communications with RADIUS servers and other applications.	
Examples	This example shows how to configure the call station ID type to use the IP address: > config radius callStationIdType ipAddr	
	This example shows how to configure the call station ID type to use the system's MAC address: > config radius callStationIdType macAddr	
	This example shows how to configure the call station ID type to use the access point's MAC address: > config radius callStationIdType ap-macAddr	
Related Commands	show radius summary	

config radius fallback-test

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

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

Syntax Description

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

Defaults

The default probe interval is 300.

Examples

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

```
> config radius fallback-test mode off
```

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

```
> config radius fallback-test mode passive
```

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

```
> config radius fallback-test mode active
```

Related Commands

[config advanced probe filter](#)
[config advanced probe limit](#)
[show advanced probe](#)
[show radius acct statistics](#)

config rfid auto-timeout

To configure an automatic timeout of radio frequency identification (RFID) tags, use the **config rfid auto-timeout** command.

config rfid auto-timeout {enable | disable}

Syntax Description

enable	Enables an automatic timeout.
disable	Disables an automatic timeout.

Defaults

None.

Examples

This example shows how to enable an automatic timeout of RFID tags:

```
> config rfid auto-timeout enable
```

Related Commands

show rfid summary
config rfid status
config rfid timeout

config rfid status

To configure radio frequency identification (RFID) tag data tracking, use the **config rfid status** command.

config rfid status {enable | disable}

Syntax Description

enable	Enables RFID tag tracking.
disable	Enables RFID tag tracking.

Defaults

None.

Examples

This example shows how to configure RFID tag tracking settings:

```
> config rfid status enable
```

Related Commands

show rfid summary
config rfid auto-timeout
config rfid timeout

config rfid timeout

To configure a static radio frequency identification (RFID) tag data timeout, use the **config rfid timeout** command.

config rfid timeout *seconds*

Syntax Description

<i>seconds</i>	Timeout in seconds (from 60 to 7200).

Defaults

None.

Examples

This example shows how to configure a static RFID tag data timeout of 60 seconds.

```
> config rfid timeout 60
```

Related Commands

show rfid summary
config rfid statistics

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		
enable		Globally enables detection and reporting of ad-hoc rogues.
disable		Globally disables detection and reporting of ad-hoc rogues.
external		Acknowledges the presence of the ad-hoc rogue.
<i>rogue_MAC</i>		MAC address of the ad-hoc rogue access point.
alert		Generates an SMNP trap upon detection of the ad-hoc rogue, and generates an immediate alert to the system administrator for further action.
all		Enables alerts for all ad-hoc rogue access points.
auto-contain		Contains all wired ad-hoc rogues detected by the controller.
<i>monitor_ap</i>		(Optional) IP address of the ad-hoc rogue access point.
contain		Contains the offending device so that its signals no longer interfere with authorized clients.
<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

The default for this command is **enabled** and is set to **alert**. The 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.

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

Examples

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

```
> config rogue adhoc enable
```

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

```
> config rogue adhoc alert all
```

Related Commands

[config rogue auto-contain level](#)
[show rogue ignore-list](#)
[show rogue rule detailed](#)
[show rogue rule summary](#)

config rogue ap classify

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

```
config rogue ap classify {friendly state {internal | external} ap_mac
config rogue ap classify {malicious | unclassified} state {alert | contain} ap_mac}
```

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

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

```
> config rogue ap classify friendly state internal 11:11:11:11:11:11
```

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

```
> config rogue ap classify malicious state alert 11:11:11:11:11:11
```

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

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

Defaults None.

Examples This example shows how to add a new friendly access point with MAC address 11:11:11:11:11:11 to the friendly MAC address list:

```
> 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 the Rogue Location Discovery Protocol (RLDP), use the **config rogue ap rldp** command.

```
config rogue ap rldp enable {alarm-only | auto-contain} [monitor_ap_only]
config rogue ap rldp initiate rogue_mac_address
config rogue ap rldp disable
```

Syntax Description

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

This example shows how to enable RLDP on all access points:

```
> config rogue ap rldp enable alarm-only
```

This example shows how to enable RLDP on monitor-mode access point *ap_1*:

```
> config rogue ap rldp enable alarm-only ap_1
```

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

```
> config rogue ap rldp initiate 123.456.789.000
```

This example shows how to disable RLDP on all access points:

```
> 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 is advertising your network's service set identifier (SSID), use the **config rogue ap ssid** command.

config rogue ap ssid {alarm | auto-contain}

Syntax Description

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

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

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

```
> 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

<i>seconds</i>	Value of 240 to 3600 seconds (inclusive), with a default value of 1200 seconds.

Defaults

1200 seconds.

Examples

This example shows how to set an expiration time for entries in the rogue access point and client list to 2400 seconds:

```
> config rogue ap timeout 2400
```

Related Commands

- config rogue ap classify
- config rogue ap friendly
- config rogue ap rldp
- config rogue ap ssid
- config rogue 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 auto-contain level

To configure rogue auto-containment level, use the **config rogue auto-contain level** command.

config rogue auto-contain level *level* [**monitor_ap_only**]

Syntax Description

<i>level</i>	Configures rogue auto-containment level in the range of 1 to 4.
Note	Up to 4 APs can be used to auto-contain when a rogue AP is moved to contained state through any of the auto-containment policies.
monitor_ap_only	(Optional) Configures auto-containment using only monitor AP mode.

Defaults

Level 1.

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 any of the configured autocontainment policies to start autocontainment. The policies for initiating autocontainment are rogue on wire (detected through RLDP or rogue detector AP), rogue using managed SSID, Valid client on Rogue AP, and AdHoc Rogue.



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

This example shows how to configure the auto-contain level to 3:

```
> config rogue auto-contain level 3
```

Related Commands

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

config rogue ap valid-client

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

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

Syntax Description

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

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

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

```
> 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

aaa	Configures AAA server or local database to validate whether rogue clients are valid clients.
enable	Enables the AAA server or local database to check rogue client MAC addresses for validity.
disable	Disables the AAA server or local database to check rogue client MAC addresses for validity.
alert	Configures the controller to forward an immediate alert to the system administrator for further action.
<i>ap_mac</i>	Access point MAC address.
contain	Configures the controller to contain the offending device so that its signals no longer interfere with authorized clients.
<i>client_mac</i>	MAC address of the rogue client.
<i>num_of_APs</i>	Maximum number of Cisco access points to actively contain the rogue access point (1–4).

Defaults

None.

Examples

This example shows how to enable the AAA server or local database to check MAC addresses:

```
> config rogue client aaa enable
```

This example shows how to disable the AAA server or local database from checking MAC addresses:

```
> config rogue client aaa disable
```

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

enable	Enables rogue detection on this access point.
disable	Disables rogue detection on this access point.
<i>cisco_ap</i>	Cisco access point.
all	Specifies all access points.



Note

If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Defaults

Enabled.

Usage Guidelines

Rogue detection is enabled by default for all access points joined to the controller except for OfficeExtend access points. OfficeExtend access points are deployed in a home environment and are likely to detect a large number of rogue devices.

Examples

This example shows how to enable rogue detection on the access point Cisco_AP:

```
> 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

add ap priority	Adds a rule with match any criteria and the priority that you specify.
<i>priority</i>	Priority of this rule within the list of rules.
classify	Specifies the classification of a rule.
friendly	Classifies a rule as friendly.
malicious	Classifies a rule as malicious.
<i>rule_name</i>	Rule to which the command applies, or the name of a new rule.
condition ap	Specifies the conditions for a rule that the rogue access point must meet.
set	Adds conditions to a rule that the rogue access point must meet.
delete	Removes conditions to a rule that the rogue access point must meet.
<i>condition_type</i>	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. The valid range is 1 to 10 (inclusive). • duration—Requires that the rogue access point be detected for a minimum period of time. The 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. The valid range is -95 to -50 dBm (inclusive). • ssid—Requires that the rogue access point have a specific SSID.
<i>condition_value</i>	Value of the condition. This value is dependent upon the <i>condition_type</i> . For instance, if the condition type is ssid , then the condition value is either the SSID name or all .
enable	Enables all rules or a single specific rule.
delete	Deletes all rules or a single specific rule.
disable	Deletes all rules or a single specific rule.
match	Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.
all	Specifies all rules defined.

any	Specifies any rule meeting certain criteria.
priority	Changes the priority of a specific rule and shifts others in the list accordingly.

Defaults

None.

Usage Guidelines

For your changes to be effective, you must enable the rule. You can configure up to 64 rules.

Examples

This example shows how to create a rule called **rule_1** with a priority of **1** and a classification as **friendly**:

```
> config rogue rule add ap priority 1 classify friendly rule_1
```

This example shows how to enable rule_1:

```
> config rogue rule enable rule_1
```

This example shows how to change the priority of the last command:

```
> config rogue rule priority 2 rule_1
```

This example shows how to change the classification of the last command:

```
> config rogue rule classify malicious rule_1
```

This example shows how to disable the last command:

```
> config rogue rule disable rule_1
```

This example shows how to delete SSID_2 from the user-configured SSID list in rule-5:

```
> 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

<i>ip_address</i>	Network IP address.
<i>netmask</i>	Subnet mask for the network.
<i>gateway</i>	IP address of the gateway for the route network.

Defaults

None.

Examples

This example shows how to configure a network route to a dedicated workstation IP address 10.1.1.0, subnet mask 255.255.255.0, and gateway 10.1.1.1:

```
> 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	<i>ip_address</i> Network IP address.
Defaults	None.
Examples	This example shows how to delete a route from the network IP address 10.1.1.0: <pre>> config route delete 10.1.1.0</pre>
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

1200	Specifies the supported connection speeds to 1200.
2400	Specifies the supported connection speeds to 2400.
4800	Specifies the supported connection speeds to 4800.
9600	Specifies the supported connection speeds to 9600.
19200	Specifies the supported connection speeds to 19200.
38400	Specifies the supported connection speeds to 38400.
57600	Specifies the supported connection speeds to 57600.

Defaults

9600.

Examples

This example shows how to configure a serial baud rate with the default connection speed of 9600:

```
> 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.

config serial timeout *minutes*

Syntax Description	<i>minutes</i> Timeout in minutes from 0 to 160. A value of 0 indicates no timeout.
Defaults	0 (no timeout).
Usage Guidelines	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.
Examples	This example shows how to configure the timeout of a serial port session to 10 minutes: > 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	debug	Configures timestamps in debug messages.
	log	Configures timestamps in log messages.
	datetime	Specifies to timestamp message logs with the standard date and time.
	disable	Specifies to prevent message logs being timestamped.

Defaults	Disabled.

Examples	This example shows how to configure timestamp message logs with the standard date and time:

```
> config service timestamps log datetime
```

This example shows how to prevent message logs being timestamped:

```
> config service timestamps debug disable
```

Related Commands	show logging

config sessions maxsessions

To configure the number of Telnet CLI sessions allowed by the Cisco wireless LAN controller, use the **config sessions maxsessions** command.

config sessions maxsessions *session_num*

Syntax Description	<i>session_num</i> Number of sessions from 0 to 5.
Defaults	5.
Usage Guidelines	Up to five sessions are possible while a setting of zero prohibits any Telnet CLI sessions.
Examples	This example shows how to configure the number of allowed CLI sessions to 2: > config sessions maxsessions 2
Related Commands	show sessions

config sessions timeout

To configure the inactivity timeout for Telnet CLI sessions, use the **config sessions timeout** command.

config sessions timeout *timeout*

Syntax Description	<i>timeout</i>	Timeout of Telnet session in minutes (from 0 to 160). A value of 0 indicates no timeout.

Defaults	5.

Examples	This example shows how to configure the inactivity timeout for Telnet sessions to 20 minutes: > config sessions timeout 20

Related Commands	show sessions

config slot

To configure various slot parameters, use the **config slot** command.

```
config slot slot_id {enable | disable | channel ap | chan_width | txpower ap | antenna extAntGain  
antenna_gain | rts} cisco_ap
```

Syntax Description		
	<i>slot_id</i>	Slot downlink radio to which the channel is assigned.
	enable	Enables the slot.
	disable	Disables the slot.
	channel	Configures the channel for the slot.
	ap	Configures one 802.11a Cisco access point.
	chan_width	Configures channel width for the slot.
	txpower	Configures Tx power for the slot.
	antenna	Configures the 802.11a antenna.
	extAntGain	Configures the 802.11a external antenna gain.
	<i>antenna_gain</i>	External antenna gain value in .5 dBi units (such as 2.5 dBi = 5).
	rts	Configures RTS/CTS for an AP.
	<i>cisco_ap</i>	Name of the Cisco access point on which the channel is configured.

Defaults	None.

Examples	This example shows how to enable slot 3 for the access point abc:

```
> config slot 3 enable abc
```

This example shows how to configure rts for the access point abc:

```
> config slot 2 rts abc
```

Related Commands	show mesh ap show mesh stats

Configure SNMP Commands

Use the **config snmp** commands to configure Simple Network Management Protocol (SNMP) settings.

config snmp community accessmode

To modify the access mode (read only or read/write) of an SNMP community, use the **config snmp community accessmode** command.

config snmp community accessmode {ro | rw} name

Syntax Description

ro	Specifies a read-only mode.
rw	Specifies a read/write mode.
<i>name</i>	SNMP community name.

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

This example shows how to configure read/write access mode for SNMP community:

```
> config snmp community accessmode rw private
```

Related Commands

show snmp community
config snmp community mode
config snmp community create
config snmp community delete
config snmp community ipaddr

config snmp community create

To create a new SNMP community, use the **config snmp community create** command.

config snmp community create *name*

Syntax Description

name SNMP community name. Up to 16 characters.

Defaults

None.

Usage Guidelines

Use this command to create a new community with the following default configuration

Examples

This example shows how to create a new SNMP community named test:

```
> config snmp community create test
```

Related Commands

show snmp community
config snmp community mode
config snmp community accessmode
config snmp community delete
config snmp community ipaddr

config snmp community delete

To delete an SNMP community, use the **config snmp community delete** command.

config snmp community delete *name*

Syntax Description

<i>name</i>	SNMP community name.

Defaults

None.

Examples

This example shows how to delete an SNMP community named test:

```
> config snmp community delete test
```

Related Commands

show snmp community
config snmp community mode
config snmp community accessmode
config snmp community create
config snmp community ipaddr

config snmp community ipaddr

To configure the IP address of an SNMP community, use the **config snmp community ipaddr** command.

config snmp community ipaddr *ip_address ip_mask name*

Syntax Description

<i>ip_address</i>	SNMP community IP address.
<i>ip_mask</i>	SNMP community subnet mask.
<i>name</i>	SNMP community name.

Defaults

None.

Examples

This example shows how to configure an SNMP community with the IP address 10.10.10.10, IP mask 255.255.255.0, and SNMP community named public:

```
> config snmp community ipaddr 10.10.10.10 255.255.255.0 public
```

Related Commands

show snmp community
config snmp community mode
config snmp community accessmode
config snmp community create
config snmp community delete
config snmp community 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	enable	Enables the community.
	disable	Disables the community.
	<i>name</i>	SNMP community name.

Defaults None.

Examples This example shows how to enable the SNMP community named public:

```
> config snmp community mode enable public
```

Related Commands

- show snmp community
- config snmp community accessmode
- config snmp community create
- config snmp community delete
- config snmp community ipaddr

config snmp engineID

To configure the SNMP engine ID, use the **config snmp engineID** command.

config snmp engineID {*engine_id* | **default**}

Syntax Description

<i>engine_id</i>	Engine ID in hexadecimal characters (a minimum of 10 and a maximum of 24 characters are allowed).
default	Restores the default engine ID.

Defaults

None.

Usage Guidelines

The SNMP engine ID is a unique string used to identify the device for administration purposes. You do need to specify an engine ID for the device because a default string is automatically generated using Cisco's enterprise number and the MAC address of the first interface on the device.

If you change the engine ID, then a reboot is required for the change to take effect.



Caution

If you change the value of the SNMP engine ID, then the password of the user entered on the command line is converted to an MD5 (Message-Digest algorithm 5) or SHA (Secure Hash Algorithm) security digest. This digest is based on both the password and the local engine ID. The command line password is then deleted. Because of this deletion, if the local value of the engine ID changes, the security digests of the SNMP users will become invalid, and the users will have to be reconfigured.

Examples

This example shows how to configure the SNMP engine ID with the value ffffffff:

```
> config snmp engineID ffffffff
```

Related Commands

[show snmpengineID](#)

config snmp syscontact

To set the SNMP system contact name, use the **config snmp syscontact** command.

config snmp syscontact *contact*

Syntax Description	<i>contact</i>	SNMP system contact name. The contact can be up to 31 alphanumeric characters.
Defaults	None.	
Examples	This example shows how to set the SMNP system contact named Cisco WLAN Solution_administrator: > config snmp syscontact Cisco WLAN Solution_administrator	
Related Commands	show snmpcommunity	

config snmp syslocation

To configure the SNMP system location name, use the **config snmp syslocation** command.

config snmp syslocation *location*

Syntax Description

<i>location</i>	SNMP system location name. The location can be up to 31 alphanumeric characters.

Defaults

None.

Examples

This example shows how to configure the SNMP system location name to Building_2a:

```
> config snmp syslocation Building_2a
```

Related Commands

show snmpcommunity

config snmp trapreceiver create

To configure a server to receive SNMP traps, use the **config snmp trapreceiver create** command.

config snmp trapreceiver create *name ip_address*

Syntax Description	<i>name</i>	SNMP community name. The name contain up to 16 characters.
	<i>ip_address</i>	SNMP community IP address.
Defaults	None.	
Usage Guidelines	The IP address must be valid for the command to add the new server.	
Examples	This example shows how to add a new SNMP trap receiver with the SNMP community named test and IP address 10.1.1.1: <pre>> config snmp trapreceiver create test 10.1.1.1</pre>	
Related Commands	show snmp trap	

config snmp trapreceiver delete

To delete a server from the trap receiver list, use the **config snmp trapreceiver delete** command.

config snmp trapreceiver delete *name*

Syntax Description	<i>name</i> SNMP community name. The name can contain up to 16 characters.
Defaults	None.
Examples	This example shows how to delete a server named test from the SNMP trap receiver list: <pre>> config snmp trapreceiver delete test</pre>
Related Commands	show snmp trap

config snmp trapreceiver mode

To send or disable sending traps to a selected server, use the **config snmp trapreceiver mode** command.

config snmp trapreceiver mode {enable | disable} name

Syntax Description	enable	Enables an SNMP trap receiver.
	disable	Disables an SNMP trap receiver.
	<i>name</i>	SNMP community name.

Defaults	None.

Usage Guidelines	This command enables or disables the Cisco wireless LAN controller from sending the traps to the selected server.

Examples	This example shows how to disable an SNMP trap receiver from sending traps to a server named server1: <pre>> config snmp trapreceiver mode disable server1</pre>

Related Commands	show snmp trap

config snmp v3user create

To create a version 3 SNMP user, use the **config snmp v3user create** command.

```
config snmp v3user create username {ro | rw} {none | hmacmd5 | hmacsha} {none | des | aescfb128} [auth_key] [encrypt_key]
```

Syntax Description

<i>username</i>	Version 3 SNMP username.
ro	Specifies a read-only user privilege.
rw	Specifies a read-write user privilege.
none	Specifies if no authentication is required.
hmacmd5	Specifies Hashed Message Authentication Coding Message Digest 5 (HMAC-MD5) for authentication.
hmacsha	Specifies Hashed Message Authentication Coding-Secure Hashing Algorithm (HMAC-SHA) for authentication.
none	Specifies if no encryption is required.
des	Specifies to use Cipher Block Chaining-Digital Encryption Standard (CBC-DES) encryption.
aescfb128	Specifies to use Cipher Feedback Mode-Advanced Encryption Standard-128 (CFB-AES-128) encryption.
<i>auth_key</i>	(Optional) Authentication key for the HMAC-MD5 or HMAC-SHA authentication protocol.
<i>encrypt_key</i>	(Optional) Encryption key for the CBC-DES or CFB-AES-128 encryption protocol.

Defaults

SNMP v3 username AccessMode Authentication Encryption

default Read/Write HMAC-SHA CFB-AES

Examples

This example shows how to add an SNMP username named test with read-only privileges and no encryption or authentication:

```
> config snmp v3user create test ro none none
```

Related Commands

show snmpv3user

config snmp v3user delete

To delete a version 3 SNMP user, use the **config snmp v3user delete** command.

config snmp v3user delete *username*

Syntax Description	<i>username</i> Username to delete.
Defaults	None.
Examples	This example shows how to remove an SNMP user named test: > config snmp v3user delete test
Related Commands	show snmp v3user

config snmp version

To enable or disable selected SNMP versions, use the **config snmp version** command.

config snmp version {v1 | v2 | v3} {enable | disable}

Syntax Description	v1	Specifies an SNMP version to enable or disable.
	v2	Specifies an SNMP version to enable or disable.
	v3	Specifies an SNMP version to enable or disable.
	enable	Enables a specified version.
	disable	Disables a specified version.

Defaults	All versions enabled

Examples	This example shows how to enable SNMP version v1: > config snmp version v1 enable

Related Commands	show snmpversion

Configure Spanning Tree Protocol Commands

Use the **config spanningtree** commands to configure Spanning Tree Protocol settings.

config spanningtree port mode

To turn fast or 802.1D Spanning Tree Protocol (STP) 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	off	Disables STP for the specified ports.
	802.1d	Specifies a supported port mode as 802.1D.
	fast	Specifies a supported port mode as fast.
	<i>port</i>	Port number (1 through 12 or 1 through 24).
	all	Configures all ports.

Defaults The default is that port STP is off.

Usage Guidelines When the Cisco 4400 Series Wireless LAN Controller is configured for port redundancy, STP must be disabled for all ports on the controller. STP can remain enabled on the switch connected to the controller. Entering this command allows the controller to set up STP, detect logical network loops, place redundant ports on standby, and build a network with the most efficient pathways.

Examples This example shows how to disable STP for all Ethernet ports:

```
> config spanningtree port mode off all
```

This example shows how to turn on STP 802.1D mode for Ethernet port 24:

```
> config spanningtree port mode 802.1d 24
```

This example shows how 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 Spanning Tree Protocol (STP) path cost for an Ethernet port, use the **config spanningtree port pathcost** command.

config spanningtree port pathcost {*cost* | **auto**} {*port* | **all**}

Syntax Description

<i>cost</i>	Cost in decimal as determined by the network planner.
auto	Specifies the default cost.
<i>port</i>	Port number (1 through 12 or 1 through 24), or all to configure all ports.
all	Configure all ports.

Defaults

auto.

Usage Guidelines

When the Cisco 4400 Series Wireless LAN Controller is configured for port redundancy, STP must be disabled for all ports on the controller. STP can remain enabled on the switch that is connected to the controller.

Examples

This example shows how to have the STP algorithm automatically assign a path cost for all ports:

```
> config spanningtree port pathcost auto all
```

This example shows how 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 Spanning Tree Protocol (STP) port priority, use the **config spanningtree port priority** command.

config spanningtree port priority *priority_num* *port*

Syntax Description

<i>priority_num</i>	Priority number from 0 to 255.
<i>port</i>	Port number (1 through 12 or 1 through 24).

Defaults

The default STP priority is 128.

Usage Guidelines

When the Cisco 4400 Series Wireless LAN Controller is configured for port redundancy, STP must be disabled for all ports on the controller. STP can remain enabled on the switch connected to the controller.

Examples

This example shows how 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	<i>priority_num</i> Priority number between 0 and 65535.

Defaults	The default is 32768.

Usage Guidelines	 Note When the Cisco 4400 Series Wireless LAN Controller is configured for port redundancy, STP must be disabled for all ports on the controller. STP can remain enabled on the switch connected to the 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	This example shows how to configure spanning tree values on a per switch basis with the bridge priority 40230: > 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	<i>seconds</i> Timeout in seconds (between 4 and 30).
Defaults	The default is 15.
Usage Guidelines	The value that all bridges use for forwarddelay when this bridge is acting as the root. 802.1D-1990 specifies that the range for this setting is related to the value of the 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 that is not a whole number of seconds. The default is 15. Valid values are 4 through 30 seconds.
Examples	This example shows how to configure spanning tree values on a per switch basis with the bridge timeout as 20 seconds: <pre>> config spanningtree switch forwarddelay 20</pre>
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	<i>seconds</i> STP hello time in seconds.
Defaults	The default is 15.
Usage Guidelines	All bridges use this value 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	This example shows how to configure the STP hello time to 4 seconds: <pre>> config spanningtree switch hellotime 4</pre>
Related Commands	<pre>show spanningtree switch spanningtree switch bridgepriority config spanningtree switch forwarddelay config spanningtree switch maxage config spanningtree switch mode</pre>

config spanningtree switch maxage

To set the maximum age, use the **config spanningtree switch maxage** command.

config spanningtree switch maxage *seconds*

Syntax Description

<i>seconds</i>	STP bridge maximum age in seconds.

Defaults

The default is 20.

Usage Guidelines

All bridges use this value for MaxAge when this bridge is acting as the root. 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

This example shows how to configure the STP bridge maximum age to 30 seconds:

```
> 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 (STP) on or off, use the **config spanningtree switch mode** command.

config spanningtree switch mode {enable | disable}

Syntax Description

enable	Enables STP on the switch.
disable	Disables STP on the switch.

Defaults

The default is that STP is disabled.

Usage Guidelines

Using this command allows the controller to set up STP, detect logical network loops, place redundant ports on standby, and build a network with the most efficient pathways.

Examples

This example shows how 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 boot-break

To enable or disable the breaking into boot prompt by pressing the **Esc** key at system startup, use the **config switchconfig boot-break** command.

config switchconfig boot-break {enable | disable}

Syntax Description

enable	Enables the breaking into boot prompt by pressing the Esc key at system startup.
disable	Disables the breaking into boot prompt by pressing the Esc key at system startup.

Defaults

Disabled.

Usage Guidelines

You must enable the features that are prerequisites for the Federal Information Processing Standard (FIPS) mode before enabling or disabling the breaking into boot prompt.

Examples

This example shows how to enable the breaking into boot prompt by pressing the **Esc** key at system startup:

```
> config switchconfig boot-break enable
```

Related Commands

[show switchconfig](#)
[config switchconfig flowcontrol](#)
[config switchconfig mode](#)
[config switchconfig secret-obfuscation](#)
[config switchconfig fips-prerequisite](#)
[config switchconfig strong-pwd](#)

config switchconfig fips-prerequisite

To enable or disable the features that are prerequisites for the Federal Information Processing Standard (FIPS) mode, use the **config switchconfig fips-prerequisite** command.

config switchconfig fips-prerequisite {enable | disable}

Syntax Description

enable	Enables the features that are prerequisites for the FIPS mode.
disable	Disables the features that are prerequisites for the FIPS mode.

Defaults

Disabled.

Usage Guidelines

You must configure the FIPS authorization secret before you can enable or disable the FIPS prerequisite features.

Examples

This example shows how to enable the features that are prerequisites for the FIPS mode:

```
> config switchconfig fips-prerequisite enable
```

Related Commands

[show switchconfig](#)
[config switchconfig boot-break](#)
[config switchconfig flowcontrol](#)
[config switchconfig mode](#)
[config switchconfig secret-obfuscation](#)
[config switchconfig strong-pwd](#)

config switchconfig strong-pwd

To enable or disable your controller to check the strength of newly created passwords, use the **config switchconfig strong-pwd** command.

**config switchconfig strong-pwd case-check | consecutive-check | default-check |
username-check | all-checks {enable | disable}**

Syntax Description		
case-check		Checks at least three combinations: lower-case characters, upper-case characters, digits, or special characters.
consecutive-check		Checks the occurrence of the same character three times.
default-check		Checks for default values or use of their variants.
username-check		Checks whether the username is specified or not.
all-checks		Checks all cases.
enable		Enables a strong password check for the AP and controller.
disable		Disables a strong password check for the AP and controller.

Defaults Enabled.

Examples This example shows how to enable the case check feature of the strong password check:

```
> config switchconfig strong-pwd case-check enable
```

Related Commands

- [show switchconfig](#)
- [config switchconfig boot-break](#)
- [config switchconfig flowcontrol](#)
- [config switchconfig mode](#)
- [config switchconfig fips-prerequisite](#)
- [config switchconfig secret-obfuscation](#)

config switchconfig flowcontrol

To enable or disable 802.3x flow control, use the **config switchconfig flowcontrol** command.

config switchconfig flowcontrol {enable | disable}

Syntax Description	enable	Enables 802.3x flow control.
	disable	Disables 802.3x flow control.

Defaults	Disabled.

Examples	This example shows how to enable 802.3x flow control on Cisco wireless LAN controller parameters: <pre>> config switchconfig flowcontrol enable</pre>

Related Commands	show switchconfig

config switchconfig mode

To configure Lightweight Access Port Protocol (LWAPP) transport mode for Layer 2 or Layer 3, use the **config switchconfig** command.

config switchconfig mode {L2 | L3}

Syntax Description

L2	Specifies Layer 2 as the transport mode.
L3	Specifies Layer 3 as the transport mode.

Defaults

L3

Examples

This example shows how to configure LWAPP transport mode to Layer 3:

```
> config switchconfig mode L3
```

Related Commands

[show switchconfig](#)

config switchconfig secret-obfuscation

To enable or disable secret obfuscation, use the **config switchconfig secret-obfuscation** command.

config switchconfig secret-obfuscation {enable | disable}

Syntax Description

enable	Enables secret obfuscation.
disable	Disables secret obfuscation.

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

This example shows how to enable secret obfuscation:

```
> config switchconfig secret-obfuscation enable
```

Related Commands

show switchconfig

config sysname

To set the Cisco wireless LAN controller system name, use the **config sysname** command.

config sysname *name*

Syntax Description

<i>name</i>	System name. The name can contain up to 31 alphanumeric characters.

Defaults

None.

Examples

This example shows how to configure the system named Ent_01:

```
> config sysname Ent_01
```

Related Commands

show sysinfo

Configure TACACS Commands

Use the **config tacacs** commands to configure TACACS+ settings.

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	Adds a new TACACS+ accounting server.
<i>server_index</i>	TACACS+ accounting server index (1 to 3).
<i>ip_address</i>	IP address for the TACACS+ accounting server.
<i>port</i>	Controller port used for the TACACS+ accounting server.
<i>type</i>	Type of secret key being used (ASCII or HEX).
<i>secret_key</i>	Secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.
enable	Enables a TACACS+ server.
retransmit-timeout	Changes the default retransmit timeout for the TACACS+ server.
<i>seconds</i>	Retransmit timeout (2 to 30 seconds).

Defaults

None.

Examples

This example shows how to add a new TACACS+ accounting server index 3 with the IP address 10.0.0.0, port number 10, and secret key 12345678 in ASCII:

```
> config tacacs acct add 1 10.0.0.0 10 ascii 12345678
```

This example shows how to change the default retransmit timeout of 30 seconds for the TACACS+ accounting server:

```
> config tacacs acct retransmit-timeout 30
```

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	Adds a new TACACS+ authorization server.
server_index	TACACS+ authorization server index (1 to 3).
ip_address	IP address for the TACACS+ authorization server.
port	Controller port used for the TACACS+ authorization server.
type	Type of secret key being used (ASCII or HEX).
secret_key	Secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.
enable	Enables a TACACS+ server.
retransmit-timeout	Changes the default retransmit timeout for the TACACS+ server.
seconds	Retransmit timeout (2 to 30 seconds).

Defaults

None.

Examples

This example shows how to add a new TACACS+ authorization server index 3 with the IP address 10.0.0.0, port number 4, and secret key 12345678 in ASCII:

```
> config tacacs athr add 3 10.0.0.0 4 ascii 12345678
```

This example shows how to change the default retransmit timeout of 30 seconds for the TACACS+ authorization server:

```
> config tacacs athr retransmit-timeout 30
```

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) Adds a new TACACS+ authentication server.
<i>server_index</i>	TACACS+ authentication server index (1 to 3).
<i>ip_address</i>	IP address for the TACACS+ authentication server.
<i>port</i>	Controller port used for the TACACS+ authentication server.
<i>type</i>	Type of secret key being used (ASCII or HEX).
<i>secret_key</i>	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.
<i>seconds</i>	Retransmit timeout (2 to 30 seconds).

Defaults

None.

Examples

This example shows how to add a new TACACS+ authentication server index 2 with the IP address 10.0.0.3, port number 6, and secret key 12345678 in ASCII:

```
> config tacacs auth add 2 10.0.0.3 6 ascii 12345678
```

This example shows how to change the default retransmit timeout of 30 seconds for TACACS+ authentication server:

```
> config tacacs auth retransmit-timeout 30
```

Related Commands

show run-config
show tacacs auth statistics
 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	<i>MM/DD/YY</i>	Date.
	<i>HH:MM:SS</i>	Time.

Defaults	None.

Examples	This example shows how to configure the system date to 04/04/2010 and time to 15:29:00: <pre>> config time manual 04/04/2010 15:29:00</pre>

Related Commands	show time

config time ntp

To set the Network Time Protocol (NTP), use the **config time ntp** command.

```
config time ntp {auth {enable server_index key_index | disable server_index} } | {interval
seconds} | {key-auth {add key_index md5 {ascii | hex} key_value | delete key_index} } |
{server server_index ip-address}
```

Syntax Description

auth	Configures the NTP authentication.
enable	Enables the NTP authentication.
<i>server_index</i>	NTP server index.
<i>key_index</i>	Key index between 1 and 4294967295.
disable	Disables the NTP authentication.
interval	Configures the NTP polling interval.
<i>seconds</i>	NTP polling interval in seconds (between 3600 and 604800).
key-auth	Configures the NTP authentication key.
add	Adds an NTP authentication key.
md5	Specifies the authentication protocol.
ascii	Specifies the ASCII key format (a maximum of 16 characters).
hex	Specifies the Hexadecimal key format (a maximum of 32 digits).
delete	Deletes an authentication key.
server	Configures the NTP servers.
<i>ip_address</i>	NTP server's IP address. Use 0.0.0.0 to delete the entry.

Defaults

None.

Examples

This example shows how to configure the NTP polling interval to 7000 seconds:

```
> config time ntp interval 7000
```

This example shows how to enable NTP authentication where the server index is 4 and the key index is 1:

```
> config time ntp auth enable 4 1
```

This example shows how to add an NTP authentication key of value ff where the key format is in hexadecimal characters and the key index is 1:

```
> config time ntp key-auth add 1 md5 hex ff
```

This example shows how to add an NTP authentication key of value ff where the key format is in ASCII characters and the key index is 1:

```
> config time ntp key-auth add 1 md5 ascii ciscokey
```

Related Commands

[show ntp-keys](#)

config time timezone

To configure the system time zone, use the **config time timezone** command.

config time timezone {enable | disable} delta_hours delta_mins

Syntax Description	enable	Enables daylight saving time.
	disable	Disables daylight saving time.
	<i>delta_hours</i>	Local hour difference from the Universal Coordinated Time (UCT).
	<i>delta_mins</i>	Local minute difference from UCT.

Defaults None.

Examples This example shows how to enable the daylight saving time:

```
> config time timezone enable 2 0
```

Related Commands **show time**

config time timezone location

To set the location of the time zone in order to have daylight saving time set automatically when it occurs, use the **config time timezone location** command.

config time timezone location *location_index*

Syntax Description	<i>location_index</i>	Number representing the time zone required. The time zones are as follows: • (GMT-12:00) International Date Line West • (GMT-11:00) Samoa • (GMT-10:00) Hawaii • (GMT-9:00) Alaska • (GMT-8:00) Pacific Time (US and Canada) • (GMT-7:00) Mountain Time (US and Canada) • (GMT-6:00) Central Time (US and Canada) • (GMT-5:00) Eastern Time (US and Canada) • (GMT-4:00) Atlantic Time (Canada) • (GMT-3:00) Buenos Aires (Argentina) • (GMT-2:00) Mid-Atlantic • (GMT-1:00) Azores • (GMT) London, Lisbon, Dublin, Edinburgh (default value) • (GMT +1:00) Amsterdam, Berlin, Rome, Vienna • (GMT +2:00) Jerusalem • (GMT +3:00) Baghdad • (GMT +4:00) Muscat, Abu Dhabi • (GMT +4:30) Kabul • (GMT +5:00) Karachi, Islamabad, Tashkent • (GMT +5:30) Colombo, Kolkata, Mumbai, New Delhi • (GMT +5:45) Katmandu • (GMT +6:00) Almaty, Novosibirsk • (GMT +6:30) Rangoon • (GMT +7:00) Saigon, Hanoi, Bangkok, Jakarta • (GMT +8:00) Hong Kong, Beijing, Chongqing • (GMT +9:00) Tokyo, Osaka, Sapporo • (GMT +9:30) Darwin • (GMT+10:00) Sydney, Melbourne, Canberra • (GMT+11:00) Magadan, Solomon Is., New Caledonia • (GMT+12:00) Kamchatka, Marshall Is., Fiji • (GMT+12:00) Auckland (New Zealand)
Defaults	None.	

Examples

This example shows how to set the location of the time zone in order to set the daylight saving time to location index 10 automatically:

```
> config time timezone location 10
```

Related Commands

[show time](#)

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

enable	Enables sending 802.11 security-related traps.
disable	Disables sending 802.11 security-related traps.

Defaults

Enabled.

Examples

This example shows how to disable the 802.11 security related traps:

```
> config trapflags 802.11-Security wepDecryptError disable
```

Related Commands

[show trapflags](#)

config trapflags aaa

To enable or disable the sending of AAA server-related traps, use the **config trapflags aaa** command.

config trapflags aaa {auth | servers} {enable | disable}

Syntax Description	auth	Enables trap sending when an AAA authentication failure occurs for management user, net user, or MAC filter.
	servers	Enables trap sending when no RADIUS servers are responding.
	enable	Enables the sending of AAA server-related traps.
	disable	Disables the sending of AAA server-related traps.

Defaults Enabled.

Examples This example shows how to enable the sending of AAA server-related traps:

```
> config trapflags aaa auth enable
```

Related Commands [show trapflags](#)

config trapflags ap

To enable or disable the sending of Cisco lightweight access point traps, use the **config trapflags ap** command.

config trapflags ap {register | interfaceUp} {enable | disable}

Syntax Description	register	Enables sending a trap when a Cisco lightweight access point registers with Cisco switch.
	interfaceUp	Enables sending a trap when a Cisco lightweight access point interface (A or B) comes up.
	enable	Enables sending access point-related traps.
	disable	Disables sending access point-related traps.

Defaults Enabled.

Examples This example shows how to prevent traps from sending access point-related traps:

```
> config trapflags ap register disable
```

Related Commands [show trapflags](#)

config trapflags authentication

To enable or disable sending traps with invalid SNMP access, use the **config trapflags authentication** command.

config trapflags authentication {enable | disable}

Syntax Description

enable	Enables sending traps with invalid SNMP access.
disable	Disables sending traps with invalid SNMP access.

Defaults

Enabled.

Examples

This example shows how to prevent sending traps on invalid SNMP access:

```
> config trapflags authentication disable
```

Related Commands

[show trapflags](#)

config trapflags client

To enable or disable the sending of client-related DOT11 traps, use the **config trapflags client** command.

```
config trapflags client {802.11-disassociate | 802.11-deauthenticate | 802.11-authfail |
                        802.11-assocfail | excluded} {enable | disable}
```

Syntax Description		
802.11-disassociate		Enables the sending of Dot11 disassociation traps to clients.
802.11-deauthenticate		Enables the sending of Dot11 deauthentication traps to clients.
802.11-authfail		Enables the sending of Dot11 authentication fail traps to clients.
802.11-assocfail		Enables the sending of Dot11 association fail traps to clients.
excluded		Enables the sending of excluded trap to clients.
enable		Enables sending of client-related DOT11 traps.
disable		Disables sending of client-related DOT11 traps.

Defaults Disabled.

Examples This example shows how to enable the sending of Dot11 disassociation trap to clients:

```
> config trapflags client 802.11-disassociate enable
```

Related Commands [show trapflags](#)

config trapflags configsave

To enable or disable the sending of configuration-saved traps, use the **config trapflags configsave** command.

config trapflags configsave {enable | disable}

Syntax Description

enable	Enables sending of configuration-saved traps.
disable	Disables the sending of configuration-saved traps.

Defaults

Enabled.

Examples

This example shows how to enable the sending of configuration-saved traps:

```
> config trapflags configsave enable
```

Related Commands

[show trapflags](#)

config trapflags IPsec

To enable or disable the sending of IPsec traps, use the **config trapflags IPsec** command.

```
config trapflags IPsec {esp-auth | esp-reply | invalidSPI | ike-neg | suite-neg | invalid-cookie}
                        {enable | disable}
```

Syntax Description

esp-auth	Enables the sending of IPsec traps when an ESP authentication failure occurs.
esp-reply	Enables the sending of IPsec traps when an ESP replay failure occurs.
invalidSPI	Enables the sending of IPsec traps when an ESP invalid SPI is detected.
ike-neg	Enables the sending of IPsec traps when an IKE negotiation failure occurs.
suite-neg	Enables the sending of IPsec traps when a suite negotiation failure occurs.
invalid-cookie	Enables the sending of IPsec traps when a Isakamp invalid cookie is detected.
enable	Enables sending of IPsec traps.
disable	Disables sending of IPsec traps.

Defaults

Enabled.

Examples

This example shows how to enable the sending of IPsec traps when ESP authentication failure occurs:

```
> config trapflags IPsec esp-auth enable
```

Related Commands

[show trapflags](#)

config trapflags linkmode

To enable or disable Cisco wireless LAN controller level link up/down trap flags, use the **config trapflags linkmode** command.

config trapflags linkmode {enable | disable}

Syntax Description

enable	Enables Cisco wireless LAN controller level link up/down trap flags.
disable	Disables Cisco wireless LAN controller level link up/down trap flags.

Defaults

Enabled.

Examples

This example shows how to enable the Cisco wireless LAN controller level link up/down trap:

```
> config trapflags linkmode disable
```

Related Commands

[show trapflags](#)

config trapflags multiusers

To enable or disable the sending of traps when multiple logins are active, use the **config trapflags multiusers** command.

```
config trapflags multiusers {enable | disable}
```

Syntax Description	enable	Enables the sending of traps when multiple logins are active.
	disable	Disables the sending of traps when multiple logins are active.

Defaults Enabled.

Examples This example shows how to disable the sending of traps when multiple logins are active:
> **config trapflags multiusers disable**

Related Commands [show trapflags](#)

config trapflags rogueap

To enable or disable sending rogue access point detection traps, use the **config trapflags rogueap** command.

config trapflags rogueap {enable | disable}

Syntax Description

enable	Enables the sending of rogue access point detection traps.
disable	Disables the sending of rogue access point detection traps.

Defaults

Enabled

Examples

This example shows how to disable the sending of rogue access point detection traps:

```
> config trapflags rogueap disable
```

Related Commands

[config rogue ap classify](#)
[config rogue ap friendly](#)
[config rogue ap rldp](#)
[config rogue ap ssid](#)
[config rogue ap timeout](#)
[config rogue ap valid-client](#)
[show rogue ap clients](#)
[show rogue ap detailed](#)
[show rogue ap summary](#)
[show rogue ap friendly summary](#)
[show rogue ap malicious summary](#)
[show rogue ap unclassified summary](#)
[show trapflags](#)

config trapflags rrm-params

To enable or disable the sending of Radio Resource Management (RRM) parameters traps, use the **config trapflags rrm-params** command.

```
config trapflags rrm-params {tx-power | channel | antenna} {enable | disable}
```

Syntax Description	tx-power	Enables trap sending when the RF manager automatically changes the tx-power level for the Cisco lightweight access point interface.
	channel	Enables trap sending when the RF manager automatically changes the channel for the Cisco lightweight access point interface.
	antenna	Enables trap sending when the RF manager automatically changes the antenna for the Cisco lightweight access point interface.
	enable	Enables the sending of RRM parameter-related traps.
	disable	Disables the sending of RRM parameter-related traps.

Defaults Enabled.

Examples This example shows how to enable the sending of RRM parameter-related traps:
> config trapflags rrm-params tx-power enable

Related Commands [show trapflags](#)

config trapflags rrm-profile

To enable or disable the sending of Radio Resource Management (RRM) profile-related traps, use the **config trapflags rrm-profile** command.

config trapflags rrm-profile {load | noise | interference | coverage} {enable | disable}

Syntax Description	load	Enables trap sending when the load profile maintained by the RF manager fails.
	noise	Enables trap sending when the noise profile maintained by the RF manager fails.
	interference	Enables trap sending when the interference profile maintained by the RF manager fails.
	coverage	Enables trap sending when the coverage profile maintained by the RF manager fails.
	enable	Enables the sending of RRM profile-related traps.
	disable	Disables the sending of RRM profile-related traps.

Defaults Enabled.

Examples This example shows how to disable the sending of RRM profile-related traps:

```
> config trapflags rrm-profile load disable
```

Related Commands [show trapflags](#)

config trapflags stpmode

To enable or disable the sending of spanning tree traps, use the **config trapflags stpmode** command.

config trapflags stpmode {enable | disable}

Syntax Description

enable	Enables the sending of spanning tree traps.
disable	Disables the sending of spanning tree traps.

Defaults

Enabled.

Examples

This example shows how to disable the sending of spanning tree traps:

```
> 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

enable	Enables WPS trap sending.
disable	Disables WPS trap sending.

Defaults

Enabled.

Examples

This example shows how to disable the WPS traps sending:

```
> 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	mac <i>MAC</i>	Specifies the MAC address of the wireless LAN.
	username <i>username</i>	Specifies the name of the user to watch.

Defaults	None.

Examples	This example shows how to add a watchlist entry for the MAC address a5:6b:ac:10:01:6b: <pre>> config watchlist add mac a5:6b:ac:10:01:6b</pre>

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

mac <i>MAC</i>	Specifies the MAC address of the wireless LAN to delete from the list.
username <i>username</i>	Specifies the name of the user to delete from the list.

Defaults

None.

Examples

This example shows how to delete a watchlist entry for the MAC address **a5:6b:ac:10:01:6b**:

```
> config watchlist delete mac a5:6b:ac:10:01:6b
```

Related Commands

[config watchlist delete](#)
[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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to disable the client watchlist: <pre>> config watchlist disable</pre>

Related Commands	config watchlist add config watchlist disable 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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to enable a watchlist entry: > 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

enable	Enables a wireless LAN.
disable	Disables a wireless LAN.
create	Creates a wireless LAN.
delete	Deletes a wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>name</i>	(Optional) WLAN profile name up to 32 alphanumeric characters.
foreignAp	(Optional) Specifies the third-party access point settings.
<i>ssid</i>	SSID (network name) up to 32 alphanumeric characters.
all	(Optional) Specifies 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

This example shows how to enable wireless LAN identifier 16:

```
> config wlan enable 16
```

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	ap-cac-limit	Supports phones that require client-controlled Call Admission Control (CAC) that expect the Cisco vendor-specific information element (IE).
	client-cac-limit	Supports phones that require access point-controlled CAC that expect the IEEE 802.11e Draft 6 QBSS-load.
	enable	Enables phone support.
	disable	Disables phone support.
	<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 This example shows how to enable the phone support that requires client-controlled CAC with wireless LAN ID 8:

```
> 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

allow	Allows 802.11e-enabled clients on the wireless LAN.
disable	Disables 802.11e on the wireless LAN.
require	Requires 802.11e-enabled clients on the wireless LAN.
<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 a multimedia capability.

Examples

This example shows how to allow 802.11e on the wireless LAN with LAN ID 1:

```
> config wlan 802.11e allow 1
```

Related Commands

[show trapflags](#)

config wlan aaa-override

To configure a user policy override via AAA on a wireless LAN, use the **config wlan aaa-override** command.

config wlan aaa-override {enable | disable} {wlan_id | foreignAp}

Syntax Description

enable	Enables policy override.
disable	Disables policy override.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies 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 VLAN to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system will also use QoS, DSCP, 802.1p priority tag values, and ACLs provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as Identity Networking.)

If the corporate wireless LAN 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 controller authentication parameter settings, and authentication is performed by the AAA server if the controller wireless LAN does not contain any client-specific authentication parameters.

The AAA override values may come from a RADIUS server, for example.

Examples

This example shows how to configure user policy override via AAA on wireless LAN ID 1:

```
> 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	<i>wlan_id</i>	Wireless LAN identifier (1 to 512).
	<i>acl_name</i>	(Optional) ACL name.
	none	(Optional) Clears the ACL settings for the specified wireless LAN.

Defaults	None.

Examples	This example shows how to configure a WLAN access control list with WLAN ID 1 and ACL named office_1: <pre>> config wlan acl 1 office_1</pre>

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 | interface_group_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

add	Creates 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>	(Optional) Interface to which you want to map the access point group.
<i>interface_group_name</i>	(Optional) Interface group to which you want to map the access point group.
delete	Removes a wireless LAN from an access point group.
description	Describes an access point group.
<i>description</i>	Description of the access point group.
interface-mapping	Assigns or removes a Wireless LAN from an access point group.
nac	Enables or disables Network Admission Control (NAC) out-of-band support on an access point group.
enable	Turns on NAC out-of-band support on an access point group.
disable	Turns 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

This example shows how to enable the NAC out-of band support on access point group 4:

```
> 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 band-select

To override the global band select configuration and enable or disable band selection on a particular WLAN, use the **config wlan band-select** command.

```
config wlan band-select allow {enable | disable} wlan_id
```

Syntax Description	config	Configuration settings.
	wlan	Wireless LAN settings.
	band-select allow	Band selection mode.
	enable	Enables band selection on a wireless LAN.
	disable	Disables band selection on a wireless LAN.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults Enabled.

Examples The following example shows you how to disable the band selection for wireless LAN ID 3.

```
> config wlan band-select allow disable 3
```

Related Commands [config band-select](#)

config wlan broadcast-ssid

To configure an Service Set Identifier (SSID) broadcast on a wireless LAN, use the **config wlan broadcast-ssid** command.

```
config wlan broadcast-ssid {enable | disable} wlan_id
```

Syntax Description	enable	Enables SSID broadcasts on a wireless LAN.
	disable	Disables SSID broadcasts on a wireless LAN.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults Disabled.

Examples This example shows how to configure an SSID broadcast on wireless LAN ID 1:
> config wlan broadcast-ssid enable 1

Related Commands [show wlan](#)

config wlan call-snoop

To enable or disable Voice-over-IP (VoIP) snooping for a particular WLAN, use the **config wlan call-snoop** command.

config wlan call-snoop {enable | disable} wlan_id

Syntax Description	enable	Enables VoIP snooping on a wireless LAN.
	disable	Disables VoIP snooping on a wireless LAN.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default	None.

Usage Guidelines	WLAN should be with Platinum QoS and it needs to be disabled while invoking this CLI

Examples	This example shows how to enable VoIP snooping for WLAN 3: <pre>> config wlan call-snoop 3 enable</pre>

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

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
enable	Enables SSID broadcasts on a wireless LAN.
disable	Disables SSID broadcasts on a wireless LAN.

Command Default

None.

Examples

This example shows how to enable CHD for WLAN 3:

```
> 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

enable	Enables the Aironet information elements.
disable	Disables the Aironet information elements.

Command Default

None.

Examples

This example shows how to enable Aironet information elements for a WLAN:

```
> config wlan ccx aironet-ie enable
```

Related Commands

[config wlan](#)
[config wlan security ckip](#)
[show client detail](#)

config wlan channel-scan defer-priority

To configure the controller to defer priority markings for packets that can defer off channel scanning, use the **config wlan channel-scan defer-priority** command.

config wlan channel-scan defer-priority *priority* [**enable** | **disable**] *wlan_id*

Syntax Description

<i>priority</i>	User priority value (0 to 7).
enable	(Optional) Enables packet at given priority to defer off channel scanning.
disable	(Optional) Disables packet at given priority to defer off channel scanning.
<i>wlan_id</i>	Wireless LAN identifier (1 to 512).

Command Default

None.

Usage Guidelines

The priority value should be set to 6 on the client and on the WLAN.

Examples

This example shows how to enable the controller to defer priority markings that can defer off channel scanning with user priority value 6 and WLAN id 30:

```
> config wlan channel-scan defer-priority 6 enable 30
```

Related Commands

[config wlan](#)
[config wlan channel-scan defer-time](#)
[show client detail](#)

config wlan channel-scan defer-time

To assign the channel scan defer time in milliseconds, use the **config wlan channel-scan defer-time** command.

config wlan channel-scan defer-time *msecs wlan_id*

Syntax Description	<i>msecs</i>	Deferral time in milliseconds (0 to 60000 milliseconds).
	<i>wlan_id</i>	Wireless LAN identifier (1 to 512).

Command Default	None.

Usage Guidelines	The time value in milliseconds should match the requirements of the equipment on your wlan.

Examples	This example shows how to assign the scan defer time to 40 milliseconds for WLAN id 50: <pre>> config wlan channel-scan defer-time 40 50</pre>

Related Commands	config wlan config wlan channel-scan defer-priority 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

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>ip_address</i>	IP address of the internal DHCP server (this parameter is required).
required	(Optional) Specifies 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

This example shows how to configure an IP address 10.10.2.1 of the internal DHCP server for wireless LAN ID 16:

```
> 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

enable	(Optional) Enables the wireless LAN diagnostic channel.
disable	(Optional) Disables the wireless LAN diagnostic channel.
<i>wlan_id</i>	Wireless LAN identifier (1 to 512).

Defaults

None.

Examples

This example shows how to enable the wireless LAN diagnostic channel for WLAN ID 1:

```
> config wlan diag-channel enable 1
```

Related Commands

[show run-config](#)
[show wlan](#)

config wlan dtim

To configure a Delivery Traffic Indicator Message (DTIM) for 802.11 radio network **config wlan dtim** command.

```
config wlan dtim {802.11a | 802.11b} dtim wlan_id
```

Syntax Description

802.11a	Configures DTIM for the 802.11a radio network.
802.11b	Configures DTIM for the 802.11b radio network.
<i>dtim</i>	Value for DTIM (between 1 to 255 inclusive).
<i>wlan_id</i>	Number of the WLAN to be configured.

Defaults

The default is DTIM 1.

Examples

This example shows how to configure DTIM for 802.11a radio network with DTIM value 128 and WLAN ID 1:

```
> 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>	Wireless LAN identifier (1 to 512).
enabled	(Optional) Enables the exclusion list for the specified wireless LAN or foreign access point.
disabled	(Optional) Disables the exclusion list for the specified wireless LAN or a foreign access point.
<i>time</i>	(Optional) 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 the **config wlan blacklist** command.

Examples

This example shows how to enable the exclusion list for WLAN ID 1:

```
> config wlan exclusionlist 1 enabled
```

Related Commands

[show wlan](#)
show wlan summary

config wlan h-reap ap-auth

To configure local authentication of clients associated with an H-REAP on a locally switched WLAN, use the **config wlan h-reap ap-auth** command.

config wlan h-reap ap-auth *wlan_id* {**enable** | **disable**}

Syntax Description

ap-auth	Configures local authentication of clients associated with an H-REAP on a locally switched WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
enable	Enables AP authentication on a WLAN.
disable	Disables AP authentication on a WLAN.

Defaults

None.

Usage Guidelines

Local switching must be enabled on the WLAN where you want to configure local authentication of clients associated with an H-REAP.

Examples

This example shows how to enable authentication of clients associated with an H-REAP on a specified WLAN:

```
> config wlan h-reap ap-auth 6 enable
```

Related Commands

[config wlan h-reap local-switching](#)
[show wlan](#)

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

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
enable	Enables client IP address learning on a wireless LAN.
disable	Disables client IP address learning on a wireless LAN.

Defaults

Disabled when the [config wlan h-reap local-switching](#) command is disabled.
Enabled when the [config wlan h-reap local-switching](#) command is enabled.

Usage Guidelines

If the client is configured with Layer 2 encryption, the controller cannot learn the client IP address, and the controller will periodically drop the client. Disable this option to keep the client connection without waiting to learn the client IP address.



Note The ability to disable IP address learning is not supported with H-REAP *central* switching.

Examples

This example shows how to disable client IP address learning for WLAN 6:

```
> 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	enable	Enables local switching on a wireless LAN.
	disable	Disables local switching on a wireless LAN.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults Disabled.

Usage Guidelines When you enable the **config wlan h-reap local-switching** command, 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 This example shows how to enable WLAN 6 for local switching:
> **config wlan h-reap local-switching enable 6**

Related Commands [config wlan h-reap learn-ipaddr](#)
[config wlan h-reap ap-auth](#)
[show wlan](#)

config wlan interface

To configure a wireless LAN interface or an interface group, use the **config wlan interface** command.

config wlan interface {*wlan_id* | **foreignAp**} *interface-name* | *interface-group-name*

Syntax Description	<i>wlan_id</i>	(Optional) Wireless LAN identifier (1 to 512)
	foreignAp	Specifies third-party access points.
	<i>interface-name</i>	Interface name.
	<i>interface-group-name</i>	Interface group name.

Defaults None.

Examples This example shows how to configure an interface named VLAN901:

```
> 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	enable	Enables IPv6 support on a wireless LAN.
	disable	Disables IPv6 support on a wireless LAN.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults	None.

Examples	This example shows how to enable WLAN 6 for local switching: > config wlan IPv6Support enable 6

Related Commands	show wlan

config wlan ldap

To add or delete a link to a configured Lightweight Directory Access Protocol (LDAP) server, use the **config wlan ldap** command.

```
config wlan ldap {add wlan_id server_id | delete wlan_id {all | server_id}}
```

Syntax Description

add	Adds a link to a configured LDAP server.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>server_id</i>	LDAP server index.
delete	Removes the link to a configured LDAP server.
all	Specifies 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

This example shows how to add a link to a configured LDAP server with the WLAN ID 100 and server ID 4:

```
> config wlan ldap add 100 4
```

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, use the **config wlan load-balance** command.

config wlan load-balance allow {enable | disable} wlan_id

Syntax Description

enable	Enables band selection on a wireless LAN.
disable	Disables band selection on a wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

Enabled.

Examples

This example shows how to enable band selection on a wireless LAN with WLAN ID 3:

```
> config wlan load-balance allow enable 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	enable	Enables MAC filtering on a wireless LAN.
	disable	Disables MAC filtering on a wireless LAN.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	foreignAp	Specifies third-party access points.

Defaults None.

Examples This example shows how to enable the MAC filtering on WLAN ID 1:
> **config wlan mac-filtering enable 1**

Related Commands [show wlan](#)

config wlan max-associated-clients

To configure the maximum number of client connections on a wireless LAN, guest LAN, or remote LAN, use the **config wlan max-associated-clients** command.

config wlan max-associated-clients *max_clients* *wlan_id*

Syntax Description

<i>max_clients</i>	Specifies the maximum number of client connections to be accepted.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to specify the maximum number of client connections on WLAN ID 2:

```
> config wlan max-associated-clients 25 2
```

Related Commands

[show wlan](#)

config wlan media-stream

To configure multicast-direct for a wireless LAN media stream, use the **config wlan media-stream** command.

config wlan media-stream multicast-direct {wlan_id | all} {enable | disable}

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
all	Configures the wireless LAN on all media streams.
enable	Enables global multicast to unicast conversion.
disable	Disables global multicast to unicast conversion.

Defaults

None.

Usage Guidelines

Media stream multicast-direct requires load based Call Admission Control (CAC) to run. WLAN quality of service (QoS) needs to be set to either gold or platinum.

Examples

This example shows how to enable the global multicast-direct media stream with WLAN ID 2:

```
> config wlan media-stream multicast-direct 2 enable
```

Related Commands

[config wlan](#)
[config wlan qos](#)
[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		Configures client MFP for the wireless LAN.
enable		(Optional) Enables the feature.
disable		(Optional) Disables the feature.
wlan_id		Wireless LAN identifier (1 to 512).
infrastructure protection		(Optional) Configures the infrastructure MFP for the wireless LAN.

Defaults	None.

Examples	This example shows how to configure client management frame protection for WLAN ID 1: <pre>> config wlan mfp client enable 1</pre>

Related Commands	show run-config 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

add	Enables MAC filtering on a wireless LAN.
delete	Disables MAC filtering on a wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>ip_address</i>	Member switch IP address for anchoring the wireless LAN.

Defaults

None.

Examples

This example shows how to configure the mobility wireless LAN anchor list with WLAN ID 4 and IP address 192.168.0.14:6:

```
> 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 mobility foreign-map](#)

config wlan mobility foreign-map

To configure interfaces or interface groups for foreign controllers, use the **config wlan mobility foreign-map** command.

```
config wlan mobility foreign-map {add | delete} wlan_id foreign_mac_address {interface_name
| interface_group_name}
```

Syntax Description

add	Adds an interface or interface group to the map of foreign controllers.
delete	Deletes an interface or interface group from the map of foreign controllers.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>foreign_mac_address</i>	Foreign switch MAC address on WLAN.
<i>interface_name</i>	Interface name up to 32 alphanumeric characters.
<i>interface_group_name</i>	Interface group name up to 32 alphanumeric characters.

Defaults

None.

Examples

This example shows how to add an interface group for foreign controllers with WLAN ID 4 and a foreign switch MAC address on WLAN 00:21:1b:ea:36:60:

```
> config wlan mobility foreign-map add 4 00:21:1b:ea:36:60 mygroup1
```

Related Commands

[show mobility foreign-map](#)
[config mobility group member](#)
[config wlan mobility anchor](#)
[debug mobility](#)
[show mobility anchor](#)
[show mobility summary](#)

config wlan multicast interface

To configure a multicast interface for a wireless LAN, use the **config wlan multicast interface** command.

config wlan multicast interface *wlan_id* {**enable** | **disable**} *interface_name*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
enable	Enables multicast interface feature for a wireless LAN.
delete	Disables multicast interface feature on a wireless LAN.
<i>interface_name</i>	Interface name.
Note The interface name can only be specified in lower case characters.	

Defaults

Multicast is disabled.

Examples

This example shows how to enable the multicast interface feature for a wireless LAN with WLAN ID 4 and interface name myinterface1:

```
> config wlan multicast interface 4 enable myinterface1
```

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 mobility foreign-map](#)

config wlan nac

To enable or disable Network Admission Control (NAC) out-of-band support for a WLAN, enter the **config wlan nac** command.

config wlan nac {snmp | radius} {enable | disable} *wlan_id*

Syntax Description

snmp	Configures SNMP NAC support.
radius	Configures RADIUS NAC support
enable	Enables NAC for the WLAN.
disable	Disables NAC for the WLAN.
<i>wlan_id</i>	WLAN identifier between 1 and 512.

Defaults

None.

Usage Guidelines

You should enable AAA override before you enable the Radius NAC state. You also should disable HREAP local switching before you enable the Radius NAC state.

Examples

This example shows how to configure SNMP NAC support for WLAN 13:

```
> config wlan nac snmp enable 13
```

This example shows how to configure RADIUS NAC support for WLAN 34:

```
> config wlan nac radius enable 20
```

Related Commands

[show nac statistics](#)
[show nac summary](#)
[config guest-lan nac](#)
[debug nac](#)

config wlan passive-client

To configure passive-client feature on a wireless LAN, use the **config wlan passive-client** command.

config wlan passive-client {enable | disable} wlan_id

Syntax Description	enable	Enables the passive-client feature on a WLAN.
	disable	Disables the passive-client feature on a WLAN.
	<i>wlan_id</i>	WLAN identifier between 1 and 512.
Defaults	None.	
Usage Guidelines	You need to enable the global multicast mode and multicast-multicast mode by using the config network multicast global and config network multicast mode commands before entering this command.	
		
Note	You should configure the multicast in multicast-multicast mode only not in unicast mode. The passive client feature does not work with multicast-unicast mode in this release.	
Examples	This example shows how to configure the passive client on wireless LAN ID 2: > config wlan passive-client enable 2	
Related Commands	config wlan config wlan config network multicast global config network multicast mode multicast show wlan	

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	disable	Disables peer-to-peer blocking and bridge traffic locally within the controller whenever possible.
	drop	Causes the controller to discard the packets.
	forward-upstream	Causes 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>	WLAN identifier between 1 and 512.

Defaults	None.

Examples	This example shows how to disable the peer-to-peer blocking for WLAN ID 1: <pre>> config wlan peer-blocking disable 1</pre>

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	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	foreignAp	Specifies third-party access points.
	bronze	Specifies the bronze QoS policy.
	silver	Specifies the silver QoS policy.
	gold	Specifies the gold QoS policy.
	platinum	Specifies the platinum QoS policy.

Defaults	Silver.

Examples	This example shows how to set the highest level of service on wireless LAN 1: <pre>> config wlan qos 1 gold</pre>

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

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
all	Configures the wireless LAN on all radio bands.
802.11a	Configures the wireless LAN on only 802.11a.
802.11bg	Configures the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled).
802.11g	Configures the wireless LAN on 802.11g only.

Defaults

None.

Examples

This example shows how to configure the wireless LAN on all radio bands:

```
> 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

auth	Configures a RADIUS authentication or accounting server.
acct	Configures a RADIUS authentication or accounting server.
enable	Enables RADIUS authentication or accounting for this WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
disable	Disables RADIUS authentication or accounting for this WLAN.
add	Adds a link to a configured RADIUS server.
<i>server_id</i>	RADIUS server index.
delete	Deletes a link to a configured RADIUS server.
all	Deletes all links to configured RADIUS servers.

Defaults

None.

Examples

This example shows how to add a link to a configured RADIUS server with WLAN ID 1 and Server ID 1:

```
> config wlan radius_server auth add 1 1
```

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 overwrite-interface

To configure a wireless LAN's RADIUS dynamic interface, use the **config wlan radius_server overwrite-interface** command.

config wlan radius_server overwrite-interface {enable | disable} wlan_id

Syntax Description

enable	Enables RADIUS dynamic interface for this WLAN.
disable	Disables RADIUS dynamic interface for this WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Usage Guidelines

The controller uses the management interface as identity. If the RADIUS server is on a directly connected dynamic interface, the traffic is sourced from the dynamic interface. Otherwise, the management IP address is used.

If the feature is enabled, controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on the WLAN.

Examples

This example shows how to enable RADIUS dynamic interface for a WLAN with an ID 1:

```
> config wlan radius_server overwrite-interface enable 1
```

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 roamed-voice-client re-anchor

To configure a roamed voice client's reanchor policy, use the **config wlan roamed-voice-client re-anchor** command:

```
config wlan roamed-voice-client re-anchor {enable | disable} wlan_id
```

Syntax Description

enable	Enables roamed client's reanchor policy.
disable	Disables roamed client's reanchor policy.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

Disabled.

Examples

This example shows how to enable a roamed voice client's reanchor policy where WLAN ID is 1:

```
> config wlan roamed-voice-client re-anchor enable 1
```

Related Commands

[show wlan](#)

config wlan sip-cac disassoc-client

To enable client disassociation in case of session initiation protocol (SIP) call admission control (CAC) failure, use this command:

```
config wlan sip-cac disassoc-client {enable | disable} wlan_id
```

Syntax Description

enable	Enables a client disassociation on a SIP CAC failure.
disable	Disables a client disassociation on a SIP CAC failure.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

Disabled.

Examples

This example shows how to enable a client disassociation on a SIP CAC failure where WLAN ID is 1:

```
> config wlan sip-cac disassoc-client enable 1
```

Related Commands

[show wlan](#)
[config wlan sip-cac send-486busy](#)

config wlan sip-cac send-486busy

To configure sending session initiation protocol (SIP) 486 busy message in case of SIP call admission control (CAC) failure, use the **config wlan sip-cac send-486busy** command:

```
config wlan sip-cac send-486busy {enable | disable} wlan_id
```

Syntax Description

enable	Enables sending SIP 486 busy on a SIP CAC failure.
disable	Disables sending SIP 486 busy on a SIP CAC failure.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

Enabled.

Examples

This example shows how to enable sending a SIP 486 busy message on a SIP CAC failure where WLAN ID is 1:

```
> config wlan sip-cac send-busy486 enable 1
```

Related Commands

[show wlan](#)
[config wlan sip-cac disassoc-client](#)

config wlan static-ip tunneling

To configure static IP client tunneling support on a WLAN, use the **config wlan static-ip tunneling** command.

config wlan static-ip tunneling {enable | disable} wlan-id

Syntax Description

tunneling	Configures static IP client tunneling support on a WLAN.
enable	Enables static IP client tunneling support on a WLAN.
disable	Disables static IP client tunneling support on a WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to enable static IP client tunneling support for WLAN ID 3:

```
> config wlan static-ip tunneling enable enable 34
```

Related Commands

[config wlan](#)
[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		
enable		Enables the 802.1X settings.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.
foreignAp		Specifies third-party access points.
disable		Disables the 802.1X settings.
0		WEP key size of 0 (no encryption) bits. The default value is 104.
		
	Note	All keys within a wireless LAN must be the same size.
40		WEP key size of 40 bits. The default value is 104.
		
	Note	All keys within a wireless LAN must be the same size.
104		WEP key size of 104 bits. The default value is 104.
		
	Note	All keys within a wireless LAN must be the same size.

Defaults None.

Usage Guidelines To change the encryption level of 802.1X security on the wireless LAN Cisco radios, use the following key sizes:

- 0—no 802.1X encryption.
- 40—40/64-bit encryption.
- 104—104/128-bit encryption. (This is the default encryption setting.)

Examples This example shows how to configure 802.1X security on WLAN ID 16:

```
> 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

enable	Enables CKIP security.
disable	Disables CKIP security.
<i>wlan_id</i>	WLAN to which you apply the command.
akm psk set-key	(Optional) Configures encryption key management for the CKIP wireless LAN.
hex	Specifies a hexadecimal encryption key.
ascii	Specifies an ASCII encryption key.
40	Sets the static encryption key length to 40 bits for the CKIP WLAN. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters.
104	Sets the static encryption key length to 104 bits for the CKIP WLAN. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.
key	Specifies the CKIP WLAN key settings.
<i>key_index</i>	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

This example shows how to configure a CKIP WLAN encryption key of 104 bits (26 hexadecimal characters) for PSK key index 2 on WLAN 03:

```
> 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, use the **config wlan security cond-web-redir** command.

config wlan security cond-web-redir {enable | disable} wlan_id

Syntax Description

enable	Enables conditional web redirect.
disable	Disables conditional web redirect.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to enable the conditional web direct on WLAN ID 2:

```
> config wlan security cond-web-redir enable 2
```

Related Commands

[show wlan](#)

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	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	foreignAp	Specifies third-party access points.

Defaults None.

Examples This example shows how to disable the IPsec for WLAN ID 16:

```
> 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

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Defaults

None.

Examples

This example shows how to enable the IPsec for WLAN ID 16:

```
> 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

hmac-md5	Specifies the IPsec HMAC-MD5 authentication protocol.
hmac-sha-1	Specifies the IPsec HMAC-SHA-1 authentication protocol.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Defaults

None.

Examples

This example shows how to configure the IPsec HMAC-SHA-1 security authentication parameter for WLAN ID 1:

```
> 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

3des	Enables IPsec 3DES encryption.
aes	Enables IPsec AES 128-bit encryption.
des	Enables IPsec DES encryption.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Defaults

None.

Examples

This example shows how to configure the IPsec aes encryption:

```
> config wlan security IPsec encryption aes 1
```

Related Commands

[show wlan](#)

config wlan security IPsec config

To configure the propriety Internet Key Exchange (IKE) CFG-Mode parameters used on the wireless LAN, use the **config wlan security IPsec config** command.

```
config wlan security IPsec config qotd ip_address {wlan_id | foreignAp}
```

Syntax Description

qotd	Configures the 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>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Defaults

None.

Usage Guidelines

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.

Examples

This example shows how to configure the quote-of-the-day server IP 44.55.66.77 for cfg-mode for WLAN 1:

```
> 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 Internet Key Exchange (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

certificates	Enables the IKE certificate mode.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
pre-share-key	Enables the IKE Xauth with preshared keys.
xauth-psk	Enables the IKE preshared key.
<i>key</i>	Key required for preshare and xauth-psk.

Defaults

None.

Examples

This example shows how to configure the IKE certification mode:

```
> config wlan security IPsec ike authentication certificates 16
```

Related Commands

[show wlan](#)

config wlan security IPsec ike dh-group

To modify the IPsec Internet Key Exchange (IKE) Diffie Hellman group used on the wireless LAN, use the **config wlan security IPsec ike dh-group** command.

config wlan security IPsec ike dh-group {*wlan_id* | **foreignAp**} {**group-1** | **group-2** | **group-5**}

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
group-1	Specifies DH group 1 (768 bits).
group-2	Specifies DH group 2 (1024 bits).
group-5	Specifies DH group 5 (1536 bits).

Defaults

None.

Examples

This example shows how to configure the Diffie Hellman group parameter for group-1:

```
> config wlan security IPsec ike dh-group 1 group-1
```

Related Commands

[show wlan](#)

config wlan security IPsec ike lifetime

To modify the IPsec Internet Key Exchange (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

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>seconds</i>	IKE lifetime in seconds, between 1800 and 345600.

Defaults

None.

Examples

This example shows how to configure the IPsec IKE lifetime use on the wireless LAN:

```
> config wlan security IPsec ike lifetime 1 1900
```

Related Commands

[show wlan](#)

config wlan security IPsec ike phase1

To modify IPsec Internet Key Exchange (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	aggressive	Enables the IKE aggressive mode.
	main	Enables the IKE main mode.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	foreignAp	Specifies third-party access points.

Defaults None.

Examples This example shows how to modify IPsec IKE Phase 1:

```
> 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

enable	Enables contivity support for this WLAN.
disable	Disables contivity support for this WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Defaults

None.

Examples

This example shows how to modify Contivity VPN client support:

```
> 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 passthru** command.

config wlan security passthru {enable | disable} {wlan_id | foreignAp} [ip_address]

Syntax Description

enable	Enables IPsec pass-through.
disable	Disables IPsec pass-through.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>ip_address</i>	(Optional) IP address of the IPsec gateway (router) that is terminating the VPN tunnel.

Defaults

None.

Examples

This example shows how to modify IPsec pass-through used on the wireless LAN:

```
> 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, use the **config wlan security splash-page-web-redir** command.

config wlan security splash-page-web-redir {enable | disable} wlan_id

Syntax Description

enable	Enables splash page web redirect.
disable	Disables splash page web redirect.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

Disabled.

Examples

This example shows how to enable splash page web redirect:

```
> config wlan security splash-page-web-redir enable 2
```

Related Commands

[show wlan](#)

config wlan security static-wep-key authentication

To configure static Wired Equivalent Privacy (WEP) key 802.11 authentication on a wireless LAN, use the **config wlan security static-wep-key authentication** command.

config wlan security static-wep-key authentication {**shared-key** | **open**} *wlan_id*

Syntax Description

shared-key	Enables shared key authentication.
open	Enables open system authentication.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to enable the static WEP shared key authentication for WLAN ID 1:

```
> config wlan security static-wep-key authentication shared-key 1
```

Related Commands

[show wlan](#)

config wlan security static-wep-key disable

To disable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key disable** command.

config wlan security static-wep-key disable *wlan_id*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to disable the static WEP keys for WLAN ID 1:

```
> 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 Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key enable** command.

config wlan security static-wep-key enable *wlan_id*

Syntax Description	<i>wlan_id</i> Wireless LAN identifier between 1 and 512.
Defaults	None.
Examples	This example shows how to enable the use of static WEK keys for WLAN ID 1: > 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 Wired Equivalent Privacy (WEP) keys and indexes, use the **config wlan security static-wep-key encryption** command.

config wlan security static-wep-key encryption *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key* *key-index*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
40	Specifies the encryption level: 40.
104	Specifies the encryption level: 104.
hex	Specifies to use hexadecimal characters to enter key.
ascii	Specifies whether to use ASCII characters to enter key.
<i>key</i>	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. Because there are only four WEP key indexes, only four wireless LANs can be configured for static WEP Layer 2 encryption.

Make sure to disable 802.1X before using this command.

Examples

This example shows how to configure the static WEP keys for WLAN ID 1 that uses hexadecimal character 0201702001 and key index 2:

```
> 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 wireless LAN, use the **config wlan security web-auth** command.

```
config wlan security web-auth {{acl | enable | disable} {wlan_id | foreignAp} [acl_name | none]}  
| {on-macfilter-failure wlan_id} | {server-precedence wlan_id [local | ldap | radius]}
```

Syntax Description		
acl		Configures the access control list.
enable		Enables web authentication.
disable		Disables web authentication.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.
foreignAp		Specifies third-party access points.
<i>acl_name</i>		ACL name (up to 32 alphanumeric characters).
none		Specifies no ACL name .
on-macfilter-failure		Enables web authentication on MAC filter failure.
server-precedence		Configures the authentication server precedence order for Web-Auth users.
local		Specifies the server type.
ldap		Specifies the server type.
radius		Specifies the server type.

Defaults None.

Examples This example shows how to configure the security policy for WLAN ID 1 and an acl named ACL03:

```
> config wlan security web-auth acl 1 ACL03
```

Related Commands [show wlan](#)

config wlan security web-passthrough acl

To add an access control list (ACL) to the wireless LAN definition, use the **config wlan security web-passthrough acl** command.

```
config wlan security web-passthrough acl {wlan_id | foreignAp} {acl_name | none}
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>acl_name</i>	ACL name (up to 32 alphanumeric characters).
none	Specifies that there is no ACL.

Defaults

None.

Examples

This example shows how to add an ACL to the wireless LAN definition:

```
> config wlan security web-passthrough acl 1 ACL03
```

Related Commands

[show wlan](#)

config wlan security web-passthrough disable

To disable a web captive portal with no authentication required on a wireless LAN, use the **config wlan security web-passthrough disable** command.

config wlan security web-passthrough disable {*wlan_id* | **foreignAp**}

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Defaults

None.

Examples

This example shows how to disable a web captive portal with no authentication required on wireless LAN ID 1:

```
> config wlan security web-passthrough disable 1
```

Related Commands

[show wlan](#)

config wlan security web-passthrough email-input

To configure a web captive portal using an e-mail address, use the **config wlan security web-passthrough email-input** command.

config wlan security web-passthrough email-input {enable | disable} {wlan_id | foreignAp}

Syntax Description

email-input	Configures a web captive portal using an e-mail address.
enable	Enables a web captive portal using an e-mail address.
disable	Disables a web captive portal using an e-mail address.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Defaults

None.

Examples

This example shows how to configure a web captive portal using an e-mail address:

```
> config wlan security web-passthrough email-input enable 1
```

Related Commands

[show wlan](#)

config wlan security web-passthrough enable

To enable a web captive portal with no authentication required on the wireless LAN, use the **config wlan security web-passthrough enable** command.

config wlan security web-passthrough enable {*wlan_id* | **foreignAp**}

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Defaults

None.

Examples

This example shows how to enable a web captive portal with no authentication required on wireless LAN ID 1:

```
> config wlan security web-passthrough enable 1
```

Related Commands

[show wlan](#)

config wlan security wpa akm 802.1x

To configure authentication key-management using 802.1x, use the **config wlan security wpa akm 802.1x** command.

config wlan security wpa akm 802.1x {enable | disable} wlan_id

Syntax Description

enable	Enables 802.1x support
disable	Disables 802.1x support
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to configure authentication using 802.1x :

```
> config wlan security wpa akm 802.1x enable 1
```

Related Commands

[show wlan](#)

config wlan security wpa akm cckm

To configure authentication key-management using Cisco Centralized Key Management (CCKM), use the **config wlan security wpa akm cckm** command.

config wlan security wpa akm cckm {**enable** *wlan_id* | **disable** *wlan_id* | *timestamp-tolerance* }

Syntax Description

enable	Enables CCKM support.
disable	Disables CCKM support.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>timestamp-tolerance</i>	Allows CCKM IE time-stamp tolerance. The range is between 1000 to 5000 milliseconds; The Default tolerance is configured as 1000 milliseconds.

Defaults

None.

Examples

This example shows how to configure authentication key-management using cckm :

```
> config wlan security wpa akm cckm 1500
```

Related Commands

[show wlan](#)

config wlan security wpa akm ft

To configure authentication key-management using 802.11r fast transition 802.1x, use the **config wlan security wpa akm ft** command.

```
config wlan security wpa akm ft [ over-the-air | over-the-ds | psk ] [ reassociation-timeout
seconds ] {enable | disable} wlan_id
```

Syntax Description

enable	Enables 802.11r fast transition 802.1x support.
disable	Disables 802.11r fast transition 802.1x support.
reassociation-timeout	Configures reassoication deadline interval.
psk	Configures 802.11r fast transition PSK support.
over-the-air	Configures 802.11r fast transition roaming Over-the-Air support.
over-the-ds	Configures 802.11r fast transition roaming DS support.
<i>seconds</i>	Reassociation deadline interval in seconds.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to configure cuthentication key-management using 802.11r fast transition :

```
> config wlan security wpa akm ft reassociation-timeout 25 1
```

Related Commands

[show wlan](#)

config wlan security wpa psk

To configure the Wi-Fi protected access (WPA) preshared key mode, use the **config wlan security wpa akm psk** command.

config wlan security wpa akm psk {enable | disable | set-key *key-format key*} *wlan_id*

Syntax Description

enable	Enables WPA-PSK.
disable	Disables WPA-PSK.
set-key	Configures pre-shared key.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>key-format</i>	Specifies key format. Either ASCII or HEX.
<i>key</i>	WPA preshared key.

Defaults

None.

Examples

This example shows how to configure the WPA preshared key mode:

```
> config wlan security wpa akm psk disable 1
```

Related Commands

[show wlan](#)

config wlan security wpa disable

To disable WPA1, use the **config wlan security wpa disable** command.

config wlan security wpa disable *wlan_id*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to disable WPA :

```
> config wlan security wpa disable 1
```

Related Commands

[show wlan](#)

config wlan security wpa enable

To enable WPA1, use the **config wlan security wpa enable** command.

config wlan security wpa enable *wlan_id*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to configure the WPA on WLAN ID 1:

```
> config wlan security wpa enable 1
```

Related Commands

[show wlan](#)

config wlan security wpa ciphers

To configure the Wi-Fi protected authentication (WPA1) or Wi-Fi protected authentication (WPA2), use the **config wlan security wpa ciphers** command.

```
config wlan security wpa { wpa1 | wpa2 } ciphers { aes | tkip } {enable | disable } wlan_id
```

Syntax Description

wpa1	Configures WPA1 support
wpa2	Configures WPA2 support
ciphers	Configure WPA ciphers
aes	Configure AES encryption support
tkip	Configure TKIP encryption support
enable	Enables WPA AES/TKIP mode.
disable	Disables WPA AES/TKIP mode.
wlan_id	Wireless LAN identifier between 1 and 512.

Defaults

None.

Usage Guidelines

If you are configuring only using the **wpa** without specifying the versions, it implies the following:

- If the cipher enabled is AES, then you are configuring WPA2/AES.
- If the ciphers enabled is AES+TKIP, then you are configuring WPA/TKIP, WPA2/AES and WPA/TKIP.
- If the cipher enabled is TKIP, then you are configuring WPA/TKIP and WPA2/TKIP.

Examples

This example shows how to encrypt the WPA:

```
> config wlan security wpa wpa1 ciphers aes enable 1
```

Related Commands

[show wlan](#)

config wlan security wpa wpa1 disable

To disable WPA1, use the **config wlan security wpa wpa1 disable** command.

config wlan security wpa wpa1 disable *wlan_id*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to disable WPA1:

```
> config wlan security wpa wpa1 disable 1
```

Related Commands

[show wlan](#)

config wlan security wpa wpa1 enable

To enable WPA1, use the **config wlan security wpa wpa1 enable** command.

config wlan security wpa wpa1 enable *wlan_id*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to enable WPA1:

```
> config wlan security wpa wpa1 enable 1
```

Related Commands

[show wlan](#)

config wlan security wpa wpa2 disable

To disable WPA2, use the **config wlan security wpa wpa2 disable** command.

config wlan security wpa wpa2 disable *wlan_id*

Syntax Description	<i>wlan_id</i> Wireless LAN identifier between 1 and 512.
Defaults	None.
Examples	This example shows how to disable WPA2: <pre>> config wlan security wpa wpa2 disable 1</pre>
Related Commands	show wlan

config wlan security wpa wpa2 enable

To enable WPA2, use the **config wlan security wpa wpa2 enable** command.

config wlan security wpa wpa2 enable *wlan_id*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Defaults

None.

Examples

This example shows how to enable WPA2:

```
> config wlan security wpa wpa2 enable 1
```

Related Commands

[show wlan](#)

config wlan session-timeout

To change the timeout of wireless LAN clients, use the **config wlan session-timeout** command.

config wlan timeout {*wlan_id* | **foreignAp**} *seconds*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>seconds</i>	Timeout or session duration in seconds.

Defaults

The default value is 1800 seconds for the following Layer 2 security types: 802.1X, Static WEP+802.1X, WPA+WPA2 with 802.1X, CCKM, or 802.1X+CCKM authentication key management; and 0 seconds for all other Layer 2 security types. A value of 0 is equivalent to no timeout.

Examples

This example shows how to configure the client timeout to 6000 seconds for WLAN ID 1:

```
> config wlan session-timeout 1 6000
```

Related Commands

[show wlan](#)

config wlan 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

<i>wlan_id</i>	Wireless LAN identifier (1 to 512).
enable	Enables web authentication exclusion.
disable	Disables web authentication exclusion.

Defaults

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

This example shows how to enable the web authentication exclusion for WLAN ID 5:

```
> 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	allow	Allows WMM on the wireless LAN.
	disable	Disables WMM on the wireless LAN.
	require	Specifies that clients use WMM on the specified wireless LAN.
	<i>wlan_id</i>	Wireless LAN identifier (1 to 512).

Defaults 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 The following example shows you how to configure wireless LAN ID 1 to allow WMM.

```
> config wlan wmm allow 1
```

The following example shows you how to configure wireless LAN ID 1 to specify that clients use WMM.

```
> config wlan wmm require 1
```

Related Commands [show run-config](#)
[show wlan](#)

Configure WPS Commands

Use the **config wps** commands to configure Wireless Protection System (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) Specifies that WMM-enabled clients are on the wireless LAN.
	<i>threshold_value</i>	Threshold value (1 to 255).

Defaults None.

Examples This example shows how to configure WMM-enabled clients with the threshold value 25:

```
> config wps ap-authentication threshold 25
```

Related Commands [show wps ap-authentication summary](#)

config wps auto-immune

To enable or disable protection from Denial of Service (DoS) attacks, use the **config wps auto-immune** command.

config wps auto-immune {enable | disable}

Syntax Description

enable	Enables the auto-immune feature.
disable	Disables the auto-immune feature.

Defaults

Disabled.

Usage Guidelines

A potential attacker can use specially crafted packets to mislead the Intrusion Detection System (IDS) into treating a legitimate client as an attacker. It causes the controller to disconnect this legitimate client and launch 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

This example shows how to configure the auto-immune mode:

```
> config wps auto-immune enable
```

Related Commands

[show wps summary](#)

config wps cids-sensor

To configure Intrusion Detection System (IDS) sensors for the Wireless Protection System (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	(Optional) Configures a new IDS sensor.
<i>index</i>	IDS sensor internal index.
<i>ip_address</i>	IDS sensor IP address.
<i>username</i>	IDS sensor username.
<i>password</i>	IDS sensor password.
delete	(Optional) Deletes an IDS sensor.
enable	(Optional) Enables an IDS sensor.
disable	(Optional) Disables an IDS sensor.
port	(Optional) Configures the IDS sensor's port number.
<i>port</i>	Port number.
interval	(Optional) Specifies the IDS sensor's query interval.
<i>query_interval</i>	Query interval setting.
fingerprint	(Optional) Specifies the IDS sensor's TLS fingerprint.
sha1	(Optional) Specifies the TLS fingerprint.
<i>fingerprint</i>	TLS fingerprint.

Defaults

Command defaults are listed below as follows:

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
Query state	Disabled

Examples

This example shows how to configure the intrusion detection system with the IDS index 1, IDS sensor IP address 10.0.0.51, IDS username Sensor_user0doc1, and IDS password passowrd01:

```
> config wps cids-sensor add 1 10.0.0.51 Sensor_user0doc1 password01
```

Related Commands

```
show wps cids-sensor detail
```

config wps client-exclusion

To 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		
802.11-assoc		Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
802.11-auth		Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
802.1x-auth		Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
ip-theft		Specifies that the control excludes clients if the IP address is already assigned to another device.
web-auth		Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
all		Specifies that the controller excludes clients for all of the above reasons.
enable		Enables client exclusion policies.
disable		Disables client exclusion policies.

Defaults All policies are enabled.

Examples This example shows how to disable clients on the 802.11 association attempt after five consecutive failures:

```
> 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	infrastructure	Configures the MFP infrastructure.
	enable	Enables the MFP feature.
	disable	Disables the MFP feature.

Defaults None.

Examples This example shows how to enable the infrastructure MFP:

```
> config wps mfp infrastructure enable
```

Related Commands [show wps mfp](#)

config wps shun-list re-sync

To force the controller to synchronization with other controllers in the mobility group for the shun list, use the **config wps shun-list re-sync** command.

config wps shun-list re-sync

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to configure the controller to synchronize with other controllers for the shun list: <pre>> config wps shun-list re-sync</pre>

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 {**standard** | **custom**} **state** *signature_id* {**enable** | **disable**}

Syntax Description

standard	Configures a standard IDS signature.
custom	Configures a standard IDS signature.
state	Specifies the state of the IDS signature.
<i>signature_id</i>	Identifier for the signature to be enabled or disabled.
enable	Enables the IDS signature processing or a specific IDS signature.
disable	Disables IDS signature processing or a specific IDS signature.

Defaults

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

This example shows how to enable IDS signature processing, which enables the processing of all IDS signatures:

```
> config wps signature enable
```

This example shows how to disable a standard individual IDS signature:

```
> 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

<i>signature_id</i>	Identifier for the signature to be configured.
<i>frequency</i>	Number of matching packets per interval that must be at the individual access point level before an attack is detected. The range is 1 to 32,000 packets per interval.

Defaults

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

This example shows how to set the number of matching packets per interval per access point before an attack is detected to 1800 for signature ID 4:

```
> 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

<i>signature_id</i>	Identifier for the signature to be configured.
<i>interval</i>	Number of seconds that must elapse before the signature frequency threshold is reached. The range is 1 to 3,600 seconds.

Defaults

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

This example shows how to set the number of seconds to elapse before reaching the signature frequency threshold to 200 for signature ID 1:

```
> 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

<i>signature_id</i>	Identifier for the signature to be configured.
<i>mac_frequency</i>	Number of matching packets per interval that must be identified per client per access point before an attack is detected. The range is 1 to 32,000 packets per interval.

Defaults

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

This example shows how to set the number of matching packets per interval per client before an attack is detected to 50 for signature ID 3:

```
> 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	<i>signature_id</i>	Identifier for the signature to be configured.
	<i>quiet_time</i>	Length of time after which no attacks have been detected at the individual access point level and the alarm can stop. The range is 60 to 32,000 seconds.

Defaults 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 This example shows how to set the number of seconds after which no attacks have been detected per access point to 60 for signature ID 1:

```
> 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

<i>signature_id</i>	Identifier for the specific IDS signature to be reset.
all	Resets all IDS signatures.

Defaults

None.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples

This example shows how to reset the IDS signature 1 to default values:

```
> 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](#)

Capwap Access Point Commands

Use the **capwap ap** commands to configure capwap access point settings.

capwap ap controller ip address

To configure the controller IP address into the capwap access point from the access point's console port, use the **capwap ap controller ip address** command.

capwap ap controller ip address *ip_address*

Syntax Description

ip_address IP address of the controller.

Defaults

None.

Usage Guidelines

This command must be entered from an access point's console port.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the controller IP address 10.23.90.81 into the capwap access point:

```
> capwap ap controller ip address 10.23.90.81
```

Related Commands

capwap ap dot1x
 capwap ap hostname
 capwap ap ip address
 capwap ap ip default-gateway
 capwap ap log-server
 capwap ap primary-base
 capwap ap primed-timer
 capwap ap secondary-base
 capwap ap tertiary-base

capwap ap dot1x

To configure the dot1x username and password into the capwap access point from the access point's console port, use the **capwap ap dot1x** command.

capwap ap dot1x username *user_name* **password** *password*

Syntax Description

<i>user_name</i>	Dot1x username.
<i>password</i>	Dot1x password.

Defaults

None.

Usage Guidelines

This command must be entered from an access point's console port.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the dot1x username ABC and password pass01:

```
> capwap ap dot1x username ABC password pass01
```

Related Commands

[capwap ap controller ip address](#)
[capwap ap hostname](#)
[capwap ap ip address](#)
[capwap ap ip default-gateway](#)
[capwap ap log-server](#)
[capwap ap primary-base](#)
[capwap ap primed-timer](#)
[capwap ap secondary-base](#)
[capwap ap tertiary-base](#)

capwap ap hostname

To configure the access point host name from the access point's console port, use the **capwap ap hostname** command.

capwap ap hostname *host_name*

Syntax Description

host_name Hostname of the access point.

Defaults

None.

Usage Guidelines

This command must be entered from an access point's console port.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the hostname WLC into the capwap access point:

```
> capwap ap hostname WLC
```

Related Commands

capwap ap controller ip address
 capwap ap dot1x
 capwap ap ip address
 capwap ap ip default-gateway
 capwap ap log-server
 capwap ap primary-base
 capwap ap primed-timer
 capwap ap secondary-base
 capwap ap tertiary-base

capwap ap ip address

To configure the IP address into the capwap access point from the access point's console port, use the **capwap ap ip address** command.

capwap ap ip address *ip_address*

Syntax Description

<i>ip_address</i>	IP address.

Defaults

None.

Usage Guidelines

This command must be entered from an access point's console port.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the IP address 10.0.0.0.1 into capwap access point:

```
> capwap ap ip address 10.0.0.1
```

Related Commands

- [capwap ap controller ip address](#)
- [capwap ap dot1x](#)
- [capwap ap hostname](#)
- [capwap ap ip default-gateway](#)
- [capwap ap log-server](#)
- [capwap ap primary-base](#)
- [capwap ap primed-timer](#)
- [capwap ap secondary-base](#)
- [capwap ap tertiary-base](#)

capwap ap ip default-gateway

To configure the default gateway from the access point's console port, use the **capwap ap ip default-gateway** command.

capwap ap ip default-gateway *default_gateway*

Syntax Description

default_gateway Default gateway address of the capwap access point.

Defaults

None.

Usage Guidelines

This command must be entered from an access point's console port.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the capwap access point with the default gateway address 10.0.0.1:

```
> capwap ap ip default-gateway 10.0.0.1
```

Related Commands

[capwap ap controller ip address](#)
[capwap ap dot1x](#)
[capwap ap hostname](#)
[capwap ap ip address](#)
[capwap ap log-server](#)
[capwap ap primary-base](#)
[capwap ap primed-timer](#)
[capwap ap secondary-base](#)
[capwap ap tertiary-base](#)

capwap ap log-server

To configure the system log server to log all the capwap errors, use the **capwap ap log-server** command.

capwap ap log-server *ip_address*

Syntax Description

<i>ip_address</i>	IP address of the syslog server.

Defaults

None.

Usage Guidelines

This command must be entered from an access point's console port.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the syslog server with the IP address 10.0.0.1:

```
> capwap ap log-server 10.0.0.1
```

Related Commands

[capwap ap controller ip address](#)
[capwap ap dot1x](#)
[capwap ap hostname](#)
[capwap ap ip address](#)
[capwap ap ip default-gateway](#)
[capwap ap primary-base](#)
[capwap ap primed-timer](#)
[capwap ap secondary-base](#)
[capwap ap tertiary-base](#)

capwap ap primary-base

To configure the primary controller name and IP address into the capwap access point from the access point's console port, use the **capwap ap primary-base** command.

capwap ap primary-base *controller_name controller_ip_address*

Syntax Description

<i>controller_name</i>	Name of the primary controller.
<i>controller_ip_address</i>	IP address of the primary controller.

Defaults

None.

Usage Guidelines

This command must be entered from an access point's console port.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the primary controller name WLC1 and primary controller IP address 10.92.109.1 into the capwap access point:

```
> capwap ap primary-base WLC1 10.92.109.1
```

Related Commands

[capwap ap controller ip address](#)
[capwap ap dot1x](#)
[capwap ap hostname](#)
[capwap ap ip address](#)
[capwap ap ip default-gateway](#)
[capwap ap log-server](#)
[capwap ap primed-timer](#)
[capwap ap secondary-base](#)
[capwap ap tertiary-base](#)

capwap ap primed-timer

To configure the primed timer into the capwap access point, use the **capwap ap primed-timer** command.

capwap ap primed-timer {enable | disable}

Syntax Description	enable	Enables the primed timer settings
	disable	Disables the primed timer settings.

Defaults None.

Usage Guidelines This command must be entered from an access point's console port.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples This example shows how to enable the primed-timer settings:

```
> capwap ap primed-timer enable
```

Related Commands

- capwap ap controller ip address
- capwap ap dot1x
- capwap ap hostname
- capwap ap ip address
- capwap ap ip default-gateway
- capwap ap log-server
- capwap ap primary-base
- capwap ap secondary-base
- capwap ap tertiary-base

capwap ap secondary-base

To configure the secondary controller name and IP address into the capwap access point from the access point's console port, use the **capwap ap secondary-base** command.

capwap ap secondary-base *controller_name controller_ip_address*

Syntax Description

<i>controller_name</i>	Name of the secondary controller.
<i>controller_ip_address</i>	IP address of the secondary controller.

Defaults

None.

Usage Guidelines

This command must be entered from an access point's console port.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the secondary controller name WLC2 and secondary controller IP address 10.92.108.2 into the capwap access point:

```
> capwap ap secondary-base WLC2 10.92.108.2
```

Related Commands

[capwap ap controller ip address](#)
[capwap ap dot1x](#)
[capwap ap hostname](#)
[capwap ap ip address](#)
[capwap ap ip default-gateway](#)
[capwap ap log-server](#)
[capwap ap primary-base](#)
[capwap ap primed-timer](#)
[capwap ap tertiary-base](#)

capwap ap tertiary-base

To configure the tertiary controller name and IP address into the capwap access point from the access point's console port, use the **capwap ap tertiary-base** command.

capwap ap tertiary-base *controller_name controller_ip_address*

Syntax Description

<i>controller_name</i>	Name of the tertiary controller.
<i>controller_ip_address</i>	IP address of the tertiary controller.

Defaults

None.

Usage Guidelines

This command must be entered from an access point's console port.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the tertiary controller name WLC3 and secondary controller IP address 10.80.72.2 into the capwap access point:

```
> capwap ap tertiary-base WLC3 10.80.72.2
```

Related Commands

[capwap ap controller ip address](#)
[capwap ap dot1x](#)
[capwap ap hostname](#)
[capwap ap ip address](#)
[capwap ap ip default-gateway](#)
[capwap ap log-server](#)
[capwap ap primary-base](#)
[capwap ap primed-timer](#)
[capwap ap secondary-base](#)

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> 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 by using the clear lwapp private-config command.
 Note	The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.
Examples	This example shows how to configure the controller IP address 10.92.109.1 into the H-REAP access point: <pre>> lwapp ap controller ip address 10.92.109.1</pre>
Related Commands	clear lwapp private-config debug lwapp console cli

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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to save the Cisco wireless LAN controller settings:

```
> save config
```

```
Are you sure you want to save? (y/n) y
```

```
Configuration Saved!
```

Related Commands	show sysinfo

Clearing Configurations, Logfiles, and Other Actions

Use the **clear** command to clear existing configurations, log files, and other functions.

clear acl counters

To clear the current counters for an access control list (ACL), use the **clear acl counters** command.

clear acl counters *acl_name*

Syntax Description	<i>acl_name</i> ACL name.
Defaults	None.
Usage Guidelines	 Note ACL counters are available only on the following controllers: Cisco 4400 Series Controller, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.
Examples	This example shows how to clear the current counters for acl1: > clear acl counters acl1
Related Commands	config acl counter show acl

clear ap-config

To clear (reset to the default values) a lightweight access point's configuration settings, use the **clear ap-config** command.

clear ap-config *ap_name*

Syntax Description

<i>ap_name</i>	Access point name.

Defaults

None.

Usage Guidelines

Entering this command does not clear the static IP address of the access point.

Examples

This example shows how to clear the access point's configuration settings for the access point named ap1240_322115:

```
> clear ap-config ap1240_322115
```

```
Clear ap-config will clear ap config and reboot the AP. Are you sure you want continue?  
(y/n)
```

Related Commands

[show ap config](#)

clear ap-eventlog

To delete the existing event log and create an empty event log file for a specific access point or for all access points joined to the controller, use the **clear ap-eventlog** command.

clear ap-eventlog {specific *ap_name* | all}

Syntax Description

specific	Specifies a specific access point log file.
<i>ap_name</i>	Name of the access point for which the event log file will be emptied.
all	Deletes the event log for all access points joined to the controller.

Defaults

None.

Examples

This example shows how to delete the event log for all access points:

```
> clear ap-eventlog all
```

```
This will clear event log contents for all APs. Do you want continue? (y/n) :y
```

```
Any AP event log contents have been successfully cleared.
```

Related Commands

[show ap eventlog](#)

clear ap join stats

To clear the join statistics for all access points or for a specific access point, use the **clear ap join stats** command.

```
clear ap join stats {all | ap_mac}
```

Syntax Description

all	Specifies all access points.
<i>ap_mac</i>	Access point MAC address.

Defaults

None.

Examples

This example shows how to clear the join statistics of all the access points:

```
> clear ap join stats all
```

Related Commands

show ap config

clear arp

To clear the Address Resolution Protocol (ARP) table, use the **clear arp** command.

clear arp

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Examples

This example shows how to clear the ARP table:

```
> clear arp
```

```
Are you sure you want to clear the ARP cache? (y/n)
```

Related Commands

clear transfer
clear download 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	802.11a	Specifies the 802.11a network.
	802.11b	Specifies the 802.11b network.
	<i>client_mac</i>	MAC address of the client.
	<i>ap_mac</i>	MAC address of a Cisco lightweight access point.
	all	Specifies all access points.

Defaults	None.

Examples	This example shows how to clear the TSM for the MAC address 00:40:96:a8:f7:98: <pre>> clear client tsm 802.11a 00:40:96:a8:f7:98 all</pre>

Related Commands	clear upload start

clear config

To reset configuration data to factory defaults, use the **clear config** command.

clear config

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to reset the configuration data to factory defaults:

```
> clear config
```

```
Are you sure you want to clear the configuration? (y/n)
```

```
n
```

```
Configuration not cleared!
```

Related Commands	clear transfer clear download 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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear the external web authentication URL: <pre>> clear ext-webauth-url</pre> 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

counters	Clears the counter statistics.
sessions	Clears the session statistics.

Defaults

None.

Examples

This example shows how to clear the license agent's counter settings:

```
> clear license agent counters
```

Related Commands

[config license agent](#)
[show license agent](#)
[license install](#)

clear location rfid

To clear a specific radio frequency identification (RFID) tag or all of the RFID tags in the entire database, use the **clear location rfid** command.

clear location rfid {*mac_address* | **all**}

Syntax Description

<i>mac_address</i>	MAC address of a specific RFID tag.
all	Specifies all of the RFID tags in the database.

Defaults

None.

Examples

This example shows how to clear all of the RFID tags in the database:

```
> clear location rfid all
```

Related Commands

[clear location statistics rfid](#)
[config location](#)
[show location](#)
[show location statistics rfid](#)

clear location statistics rfid

To clear radio frequency identification (RFID) statistics, use the **clear location statistics rfid** command.

clear location statistics rfid

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear RFID statistics: <pre>> clear location statistics rfid</pre>

Related Commands	clear location statistics rfid config location show location

clear locp statistics

To clear the Location Protocol (LOCP) statistics, use the **clear locp statistics** command.

clear locp statistics

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear the statistics related to LOCP: <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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear the login banner file: > clear login-banner

Related Commands	transfer download datatype

clear lwapp private-config

To clear (reset to default values) an access point's current Lightweight Access Point Protocol (LWAPP) private configuration, which contains static IP addressing and controller IP address configurations, use the **clear lwapp private-config** command.

clear lwapp private-config

Syntax Description	This command has no arguments or keywords.

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 by using the clear lwapp private-config command.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples	This example shows how to clear an access point's current LWAPP private configuration:

```
AP# clear lwapp private-config  
removing the reap config file flash:/lwapp_reap.cfg
```

Related Commands	debug capwap debug capwap reap debug lwapp console cli show capwap reap association show capwap reap status

clear nmsp statistics

To clear the Network Mobility Services Protocol (NMSP) statistics, use the **clear nmsp statistics** command.

clear nmsp statistics

Syntax Description This command has no arguments or keywords.

Defaults None.

Examples This example shows how to delete the NMSP statistics log file:

```
> clear nmsp statistics
```

Related Commands

- [clear locp statistics](#)
- [config nmsp notify-interval measurement](#)
- [show nmsp notify-interval summary](#)
- [show nmsp status](#)

clear radius acct statistics

To clear the RADIUS accounting statistics on the controller, use the **clear radius acc statistics** command.

clear radius acct statistics [*index* | **all**]

Syntax Description

index	(Optional) Index of the RADIUS accounting server.
all	(Optional) Specifies all RADIUS accounting servers.

Defaults

None.

Examples

This example shows how to clear the RADIUS accounting statistics:

```
> clear radius acct statistics
```

Related Commands

show radius acct statistics

clear tacacs auth statistics

To clear the RADIUS authentication server statistics in the controller, use the **clear tacacs auth statistics** command.

clear radius tacacs auth statistics [*index* | **all**]

Syntax Description

index	(Optional) Index of the RADIUS authentication server.
all	(Optional) Specifies all RADIUS authentication servers.

Defaults

None.

Examples

This example shows how to clear the RADIUS authentication server statistics:

```
> clear tacacs auth statistics
```

Related Commands

show tacacs auth statistics
show tacacs summary
config tacacs auth

clear redirect-url

To clear the custom web authentication redirect URL on the Cisco wireless LAN controller, use the **clear redirect-url** command.

clear redirect-url

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear the custom web authentication redirect URL:

```
> clear redirect-url
```

```
URL cleared.
```

Related Commands	clear transfer clear download datatype clear download filename clear download mode clear download path clear download start clear upload datatype clear upload filename clear upload mode clear upload path clear upload serverip clear upload start

clear stats ap wlan

To clear the WLAN statistics, use the **clear stats ap wlan** command.

clear stats ap wlan *cisco_ap*

Syntax Description

<i>cisco_ap</i>	Selected configuration elements.

Defaults

None.

Examples

This example shows how to clear the WLAN configuration elements of the access point *cisco_ap*:

```
> clear stats ap wlan cisco-ap
```

```
WLAN statistics cleared.
```

Related Commands

[show ap stats](#)
[show ap wlan](#)

clear stats local-auth

To clear the local Extensible Authentication Protocol (EAP) statistics, use the **clear stats local-auth** command.

clear stats local-auth

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear the local EAP statistics:

```
> clear stats local-auth
```

```
Local EAP Authentication Stats Cleared.
```

Related Commands	config local-auth active-timeout config local-auth eap-profile config local-auth method fast config local-auth user-credentials debug aaa local-auth show local-auth certificates show local-auth config show local-auth statistics

clear stats mobility

To clear mobility manager statistics, use the **clear stats mobility** command.

clear stats mobility

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear mobility manager statistics:

```
> clear stats mobility
```

```
Mobility stats cleared.
```

Related Commands	clear transfer clear download datatype clear download filename clear download mode clear download serverip clear download start clear upload datatype clear upload filename clear upload mode clear upload path clear upload serverip clear upload start clear stats port

clear stats port

To clear statistics counters for a specific port, use the **clear stats port** command.

clear stats port *port*

Syntax Description

<i>port</i>	Physical interface port number.

Defaults

None.

Examples

This example shows how to clear the statistics counters for port 9:

```
> clear stats port 9
```

Related Commands

clear transfer
clear download datatype
clear download filename
clear download mode
clear download serverip
clear download start
clear upload datatype
clear upload filename
clear upload mode
clear upload path
clear upload serverip
clear upload start

clear stats 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

<i>auth</i>	Clears statistics regarding authentication.
<i>acct</i>	Clears statistics regarding accounting.
<i>index</i>	Index number of the RADIUS server to be cleared.
<i>all</i>	Clears statistics for all RADIUS servers.

Defaults

None.

Examples

This example shows how to clear the statistics for all RADIUS authentication servers:

```
> clear stats radius auth all
```

Related Commands

clear transfer
 clear download datatype
 clear download filename
 clear download mode
 clear download serverip
 clear download start
 clear upload datatype
 clear upload filename
 clear upload mode
 clear upload path
 clear upload serverip
 clear upload start

clear stats switch

To clear all switch statistics counters on a Cisco wireless LAN controller, use the **clear stats switch** command.

clear stats switch

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear all switch statistics counters: <pre>> clear stats switch</pre>

Related Commands	<pre>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</pre>

clear stats tacacs

To clear the TACACS+ server statistics on the controller, use the **clear stats tacacs** command.

clear stats tacacs [**auth** | **athr** | **acct**] [*index* | **all**]

Syntax Description	auth	(Optional) Clears the TACACS+ authentication server statistics.
	athr	(Optional) Clears the TACACS+ authorization server statistics.
	acct	(Optional) Clears the TACACS+ accounting server statistics.
	index	Index of the TACACS+ server.
	all	(Optional) Specifies all TACACS+ servers.

Defaults	None.

Examples	This example shows how to clear the TACACS+ accounting server statistics for index 1: <pre>> clear stats tacacs acct 1</pre>

Related Commands	show tacacs summary

clear transfer

To clear the transfer information, use the **clear transfer** command.

clear transfer

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear the transfer information:

```
> clear transfer
```

```
Are you sure you want to clear the transfer information? (y/n) y
```

```
Transfer Information Cleared.
```

Related Commands	transfer upload datatype transfer upload 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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear the trap log:

```
> clear traplog
```

```
Are you sure you want to clear the trap log? (y/n) y
```

```
Trap Log Cleared.
```

Related Commands	clear transfer clear download datatype clear download filename clear download mode clear download path clear download serverip clear download start clear upload filename clear upload mode clear upload path clear upload serverip clear upload start

clear webimage

To clear the custom web authentication image, use the **clear webimage** command.

clear webimage

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear the custom web authentication image: <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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear the custom web authentication message:

```
> clear webmessage
```

```
Message cleared.
```

Related Commands	clear transfer clear download datatype clear download filename clear download mode clear download path clear download serverip clear download start clear upload filename clear upload mode clear upload path clear upload serverip clear upload start

clear webtitle

To clear the custom web authentication title, use the **clear webtitle** command.

clear webtitle

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to clear the custom web authentication title: <pre>> clear webtitle</pre> Title cleared.

Related Commands	clear transfer clear download datatype clear download filename clear download mode clear download path clear download serverip clear download start clear upload filename clear upload mode clear upload path clear upload serverip clear upload start

Resetting the System Reboot Time

Use the **reset** command to schedule a reboot of the controller and access points.

reset system at

To reset the system at a specified time, use the **reset system at** command.

reset system at YYYY-MM-DD HH: MM: SS image {no-swap | swap} reset-aps [save-config]

Syntax Description	YYYY-MM-DD	Date.
	HH: MM: SS	Time in 24-hour format.
	image	Configures the image to be rebooted.
	swap	Changes the active boot image.
	no-swap	Boots from the active image.
	reset-aps	Resets all access points during the system reset.
	save-config	(Optional) Saves the configuration before the system reset.

Defaults	None.

Examples	This example shows how to reset the system at 2010-03-29 and 12:01:01 time: <pre>> reset system at 2010-03-29 12:01:01 image swap reset-aps save-config</pre>

Related Commands	reset system notify-time reset system in

reset system in

To specify the amount of time delay before the devices reboot, use the **reset system in** command.

reset system in *HH: MM: SS* image {swap | no-swap} reset-aps save-config

Syntax Description	HH :MM :SS	Delay in duration.
	image	Configures the image to be rebooted.
	swap	Changes the active boot image
	no-swap	Boots from the active image.
	reset-aps	Resets all access points during the system reset.
	save-config	Saves the configuration before the system reset.

Defaults None.

Examples This example shows how to reset the system after a delay of 00:01:01:

```
> reset system in 00:01:01 image swap reset-aps save-config
```

Related Commands

- reset system notify-time**
- reset system at**

reset system cancel

To cancel a scheduled reset, use the **reset system cancel** command.

reset system cancel

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to cancel a scheduled reset: <pre>> reset system cancel</pre>

Related Commands	reset system at reset system in reset system notify-time

reset system notify-time

To configure the trap generation prior to scheduled resets, use the **reset system notify-time** command.

reset system notify-time *minutes*

Syntax Description	minutes	Number of minutes before each scheduled reset at which to generate a trap.

Defaults	The default is 10 minutes.

Examples	This example shows how to configure the trap generation to 10 minutes before the scheduled resets: > reset system notify-time 55

Related Commands	reset system in reset system at

Uploading and Downloading Files and Configurations

Use the **transfer** command to transfer files to or from the Cisco wireless LAN controller.

transfer download certpassword

To set the password for the .PEM file so that the operating system can decrypt the web administration SSL key and certificate, use the **transfer download certpassword** command.

transfer download certpassword *private_key_password*

Syntax Description

private_key_password Certificate's private key password.

Defaults

None.

Examples

This example shows how to transfer a file to the switch with the certificate's private key password certpassword:

```
> transfer download certpassword
```

```
Clearing password
```

Related Commands

clear transfer
transfer download filename
transfer download mode
transfer download path
transfer download serverip
transfer download start
transfer upload datatype
transfer upload filename
transfer upload mode
transfer upload path
transfer upload serverip
transfer upload start

transfer download datatype

To set the download file type, use the **transfer download datatype** command.

transfer download datatype {config | code | image | signature | webadmincert | webauthbundle | eapdevcert | eapcacert}

Syntax Description		
config		Downloads the configuration file.
code		Downloads an executable image to the system.
image		Downloads a web page login to the system.
signature		Downloads a signature file to the system.
webadmincert		Downloads a certificate for web administration to the system.
webauthbundle		Downloads a custom webauth bundle to the system.
eapdevcert		Downloads an EAP dev certificate to the system.
eapcacert		Downloads an EAP ca certificate to the system.

Defaults	None.

Examples	This example shows how to download an executable image to the system: <pre>> transfer download datatype code</pre>

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

<i>filename</i>	Filename that contains up to 512 alphanumeric characters.

Defaults

None.

Examples

This example shows how to transfer a file named build603:

```
> transfer download filename build603
```

Related Commands

clear transfer
 transfer download certpassword
transfer download mode
transfer download path
transfer download serverip
transfer download start
transfer upload datatype
transfer upload filename
transfer upload mode
transfer upload path
transfer upload serverip
transfer upload start

transfer download mode

To set the transfer mode, use the **transfer download mode** command.

transfer download mode {ftp | tftp}

Syntax Description	ftp	Sets the transfer mode to FTP.
	tftp	Sets the transfer mode to TFTP.

Defaults	None.

Examples	This example shows how to transfer a file using the tftp mode: <pre>> transfer download mode tftp</pre>

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 an FTP transfer, use the **transfer download password** command.

transfer download password *password*

Syntax Description

<i>password</i>	Password.

Defaults

None.

Examples

This example shows how to set the password for FTP transfer to pass01:

```
> transfer download password pass01
```

Related Commands

[transfer download mode](#)
[transfer download port](#)
[transfer download username](#)

transfer download path

To set a specific FTP or TFTP path, use the **transfer download path** command.

transfer download path *path*

Syntax Description	<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	This example shows how to transfer a file to the path c:\install\version2: > transfer download path c:\install\version2

Related Commands	clear transfer transfer download 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

<i>port</i>	FTP port.

Defaults

The default FTP *port* is **21**.

Examples

This example shows how to specify FTP port number 23:

```
> transfer download port 23
```

Related Commands

[transfer download mode](#)
[transfer download 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

TFTP_server	TFTP IP address.
ip_address	Server IP address.

Defaults

None.

Examples

This example shows how to configure the IP address of the TFTP server with the IP address 175.34.56.78:

```
> transfer download serverip 175.34.56.78
```

Related Commands

clear transfer
transfer download 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 This command has no arguments or keywords.

Defaults None.

Examples This example shows how to initiate a download:

```
> transfer download start
```

```
Mode..... TFTP
Data Type..... Site Cert
TFTP Server IP..... 172.16.16.78
TFTP Path..... directory path
TFTP Filename..... webadmincert_name
```

```
This may take some time.
Are you sure you want to start? (y/n) Y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

Related Commands

clear transfer
transfer download 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	<i>timeout</i> Timeout in seconds between 1 and 254.

Defaults	None.

Examples	This example shows how to transfer a file with the TFTP packet timeout of 55 seconds: > 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

<i>retries</i>	Number of allowed TFTP packet retries between 1 and 254 seconds.

Defaults

None.

Examples

This example shows how to set the number of allowed TFTP packet retries to 55:

```
> transfer download tftpMaxRetries 55
```

Related Commands

clear transfer
 transfer download 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	<i>username</i> Username.
Defaults	None.
Examples	This example shows how to set the FTP username to ftp_username: <pre>> transfer download username ftp_username</pre>
Related Commands	transfer download mode transfer download password transfer download port

transfer encrypt

To configure encryption for configuration file transfers, use the **transfer encrypt** command.

transfer encrypt {**enable** | **disable** | **set-key** *key*}

Syntax Description

enable	Enables the encryption settings.
disable	Disables the encryption settings.
set-key	Specifies the encryption key for configuration file transfers.
<i>key</i>	Encryption key for config file transfers.

Defaults

None.

Examples

This example shows how to enable the encryption settings:

```
> 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	
config	Uploads the system configuration file.
coredump	Uploads the core-dump file.
crashfile	Uploads the system crash file.
errorlog	Uploads the system error log file.
invalid-config	Uploads the system invalid-config file.
pac	Uploads a Protected Access Credential (PAC).
packet-capture	Uploads a packet capture file.
panic-crash-file	Uploads the kernel panic information file.
radio-core-dump	Uploads the system error log.
signature	Uploads the system signature file.
systemtrace	Uploads the system trace file.
traplog	Uploads the system trap log.
watchdog-crash-file	Uploads a console dump file resulting from a software-watchdog-initiated controller reboot following a crash.

Defaults None.

Examples This example shows how to upload the system error log file:

```
> transfer upload datatype errorlog
```

Related Commands

- [clear transfer](#)
- [transfer upload filename](#)
- [transfer upload mode](#)
- [transfer upload pac](#)
- [transfer upload password](#)
- [transfer upload path](#)
- [transfer upload port](#)
- [transfer upload serverip](#)
- [transfer upload start](#)
- [transfer upload username](#)

transfer upload filename

To upload a specific file, use the **transfer upload filename** command.

transfer upload filename *filename*

Syntax Description	<i>filename</i> Filename that contains up to 16 alphanumeric characters.
Defaults	None.
Examples	This example shows how to upload a file build603: <pre>> transfer upload filename build603</pre>
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	ftp	Sets the transfer mode to FTP.
	tftp	Sets the transfer mode to TFTP.

Defaults	None.

Examples	This example shows how to set the transfer mode to TFTP: <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.

transfer upload pac *username validity password*

Syntax Description

username	User identity of the PAC.
validity	Validity period (days) of the PAC.
password	Password to protect the PAC.

Defaults

None.

Usage Guidelines

The client upload process uses a TFTP or FTP server.

Examples

This example shows how to upload a PAC with the username user1, validity period 53, and password pass01:

```
> transfer upload pac user1 53 pass01
```

Related Commands

[clear transfer](#)
[transfer upload 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	<i>password</i> Password needed to access the FTP server.
Defaults	None.
Examples	This example shows how to configure the password for the FTP transfer to pass01: <pre>> transfer upload password pass01</pre>
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

<i>path</i>	Server path to file.

Defaults

None.

Examples

This example shows how to set the upload path to c:\install\version2:

```
> transfer upload path c:\install\version2
```

Related Commands

[clear transfer](#)
[transfer upload 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	<i>port</i> Port number.
Defaults	The default FTP port is 21 .
Examples	This example shows how to specify FTP port 23: <pre>> transfer upload port 23</pre>
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

<i>ip_address</i>	Server IP address.

Defaults

None.

Examples

This example shows how to set the IP address of the TFTP server to 175.31.56.78:

```
> 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	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to initiate an upload of a file:

```
> transfer upload start

Mode..... TFTP
TFTP Server IP..... 172.16.16.78
TFTP Path..... c:\find\off/
TFTP Filename..... wps_2_0_75_0.aes
Data Type..... Code

Are you sure you want to start? (y/n) n

Transfer Cancelled
```

Related Commands	clear transfer transfer upload 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

<i>username</i>	Username required to access the FTP server. The username can contain up to 31 characters.

Defaults

None.

Examples

This example shows how to set the FTP username to ftp_username:

```
> transfer upload username ftp_username
```

Related Commands

- [clear transfer](#)
- [transfer upload 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, see the “Installing and Configuring Licenses” section in Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide*.

license clear

To remove a license from the Cisco 5500 Series Controller, use the **license clear** command.

license clear *license_name*

Syntax Description

<i>license_name</i>	Name of the license.

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

This example shows how to remove the license settings of the license named wplus-ap-count:

```
> license clear wplus-ap-count
```

Related Commands

[license comment](#)
[license install](#)
[license revoke](#)
[license save](#)
[show license all](#)

license comment

To add comments to a license or delete comments from a license on the Cisco 5500 Series Controller, use the **license comment** command.

license comment {**add** | **delete**} *license_name comment_string*

Syntax Description

add	Adds a comment.
delete	Deletes a comment.
<i>license_name</i>	Name of the license.
<i>comment_string</i>	License comment.

Defaults

None.

Examples

This example shows how to add a comment “wplus ap count license” to the license name wplus-ap-count:

```
> license comment add wplus-ap-count Comment for wplus ap count license
```

Related Commands

[license clear](#)
[license install](#)
[license revoke](#)
[license save](#)
[show license all](#)

license install

To install a license on the Cisco 5500 Series Controller, use the **license install** command.

license install *url*

Syntax Description	<i>url</i> URL of the TFTP server (tftp://server_ip/path/filename).

Defaults	None.

Usage Guidelines	We recommend that the access point count be the same for the base-ap-count and wplus-ap-count licenses installed on your controller. If your controller has a base-ap-count license of 100 and you install a wplus-ap-count license of 12, the controller supports up to 100 access points when the base license is in use but only a maximum of 12 access points when the wplus license is in use.

You cannot install a wplus license that has an access point count greater than the controller's base license. For example, you cannot apply a wplus-ap-count 100 license to a controller with an existing base-ap-count 12 license. If you attempt to register for such a license, an error message appears indicating that the license registration has failed. Before upgrading to a wplus-ap-count 100 license, you would first have to upgrade the controller to a base-ap-count 100 or 250 license.

Examples	This example shows how to install a license on the controller from the URL tftp://10.10.10.10/path/license.lic:

```
> license install tftp://10.10.10.10/path/license.lic
```

Related Commands	license clear license 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

<i>license_name</i>	Ap-count evaluation license.
high	Modifies the priority of an ap-count evaluation license.
low	Modifies the priority of an ap-count evaluation license.

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, which forces the controller to use the permanent license.



Note

You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.



Note

If the ap-count evaluation license is a wplus license and the ap-count permanent license is a base license, you must also change the feature set to wplus.



Note

To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

Examples

This example shows how to set the priority of the wplus-ap-count to high:

```
> license modify priority wplus-ap-count high
```

license modify priority**Related Commands**

[license clear](#)
[license install](#)
[license revoke](#)
[license save](#)
[show license all](#)

license revoke

To rehost a license on a Cisco 5500 Series Controller, use the **license revoke** command.

license revoke {*permission_ticket_url* | **rehost** *rehost_ticket_url*}

Syntax Description	<i>permission_ticket_url</i>	URL of the TFTP server (tftp://server_ip/path/filename) where you saved the permission ticket.
	rehost	Specifies the rehost license settings.
	<i>rehost_ticket_url</i>	URL of the TFTP server (tftp://server_ip/path/filename) where you saved the rehost ticket.

Defaults None.

Usage Guidelines

Before you revoke a license, save the device credentials by using the **license save credential url** command.

You can rehost all permanent licenses except the permanent base image license. Evaluation licenses and the permanent base image license cannot be rehosted.

In order to rehost a license, you must generate credential information from the controller and use it to obtain a permission ticket to revoke the license from the Cisco licensing site (<https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet>). Next, you must obtain a rehost ticket and use it to obtain a license installation file for the controller on which you want to install the license.

For detailed information on rehosting licenses, see the “Installing and Configuring Licenses” section in Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide*.

Examples

This example shows how to revoke the license settings from the saved permission ticket URL `tftp://10.10.10.10/path/permit_ticket.lic`:

```
> license revoke tftp://10.10.10.10/path/permit_ticket.lic
```

This example shows how to revoke the license settings from the saved rehost ticket URL `tftp://10.10.10.10/path/rehost_ticket.lic`:

```
> license revoke rehost tftp://10.10.10.10/path/rehost_ticket.lic
```

Related Commands

- license clear**
- license install**
- license modify priority**
- license save**
- show license all**

license save

To save a backup copy of all installed licenses or license credentials on the Cisco 5500 Series Controller, use the **license save** command.

license save credential *url*

Syntax Description

<i>credential</i>	Saves device credential information to a file.
<i>url</i>	URL of the TFTP server (tftp://server_ip/path/filename).

Defaults

None.

Usage Guidelines

Save the device credentials before you revoke the license by using the **license revoke** command.

Examples

This example shows how to save a backup copy of all installed licenses or license credentials on tftp://10.10.10.10/path/cred.lic:

```
> license save credential tftp://10.10.10.10/path/cred.lic
```

Related Commands

license clear
license install
license 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. 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	(Optional) Specifies debugging of all AAA messages.
detail	(Optional) Specifies debugging of AAA errors.
events	(Optional) Specifies debugging of AAA events.
packet	(Optional) Specifies debugging of AAA packets.
ldap	(Optional) Specifies debugging of the AAA Lightweight Directory Access Protocol (LDAP) events.
local-auth	(Optional) Specifies debugging of the AAA local Extensible Authentication Protocol (EAP) events.
tacacs	(Optional) Specifies debugging of the AAA TACACS+ events.
enable	(Optional) Starts the debugging feature.
disable	(Optional) Stops the debugging feature.

Defaults

None.

Examples

This example shows how to enable the debugging of AAA LDAP events:

```
> 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 back-end messages and events.
	shim	Configures debugging of the AAA local authentication shim layer events.
	eap	Configures debugging of the AAA local Extensible Authentication Protocol (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	Starts the debugging feature.
	disable	Stops the debugging feature.

Defaults	None.

Examples	This example shows how to enable the debugging of the AAA local EAP authentication: <pre>> debug aaa local-auth eap method all enable</pre>

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

all	Configures debugging of all Airewave Director logs.
channel	Configures debugging of the Airewave Director channel assignment protocol.
detail	Configures debugging of the Airewave Director detail logs.
error	Configures debugging of the Airewave Director error logs.
group	Configures debugging of the Airewave Director grouping protocol.
manager	Configures debugging of the Airewave Director manager.
message	Configures debugging of the Airewave Director messages.
packet	Configures debugging of the Airewave Director packets.
power	Configures debugging of the Airewave Director power assignment protocol and coverage hole detection.
profile	Configures debugging of the Airewave Director profile events.
radar	Configures debugging of the Airewave Director radar detection/avoidance protocol.
rf-change	Configures debugging of the Airewave Director rf changes.
enable	Enables the Airewave Director debug setting.
disable	Disables the Airewave Director debug setting.

Defaults

None.

Examples

This example shows how to enable the debugging of Airewave Director profile events:

```
> debug airewave-director profile enable
```

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 the **debug ap** command.

debug ap {**enable** | **disable** | **command** *cmd*} *cisco_ap*

Syntax Description	enable	Enables debugging on a lightweight access point.
	Note	The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
	disable	Disables debugging on a lightweight access point.
	Note	The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
	command	Specifies that a CLI command is to be executed on the access point.
	<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

This example shows how to enable remote debugging on access point AP01:

```
> debug ap enable AP01
```

This example shows how to execute the **config ap location** command on access point AP02:

```
> debug ap command "config ap location "Building 1" AP02"
```

This example shows how 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 the **debug ap enable** 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 is 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

This example shows how to enable remote debugging on access point AP01:

```
> debug ap enable AP01
```

This example shows how to disable remote debugging on access point AP02:

```
> debug ap disable AP02
```

This example shows how 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 show stats

To troubleshoot video messages and statistics of Cisco lightweight access points, use the **debug ap show stats** command.

```
debug ap show stats {802.11a | 802.11b} cisco_ap {tx-queue | packet | load | multicast | client
{client_MAC | video | all} | video metrics}
```

Syntax Description		
802.11a		Specifies the 802.11a network.
802.11b		Specifies the 802.11b/g network.
cisco_ap		Cisco lightweight access point name.
tx-queue		Displays the AP's transmit queue traffic statistics.
packet		Displays the AP's packet statistics.
load		Displays the AP's QBSS and other statistics.
multicast		Displays the AP's multicast supported rate statistics.
client		Displays the specified client's metric statistics.
client_MAC		MAC address of the client.
video		Displays video statistics of all clients on the AP.
all		Displays statistics of all clients on the AP.
video metrics		Displays the video metric statistics.

Defaults

None.

Examples

This example shows how to troubleshoot the access point AP01's transmit queue traffic on an 802.11a network:

```
> debug ap show stats 802.11a AP01 tx-queue
```

This example shows how to troubleshoot the access point AP02's multicast supported rates on an 802.11b/g network:

```
> debug ap show stats 802.11b AP02 multicast
```

This example shows how to troubleshoot the metrics of a client identified by its MAC address, associated with the access point AP01 on an 802.11a network:

```
> debug ap show stats 802.11a AP01 client 00:40:96:a8:f7:98
```

This example shows how to troubleshoot the metrics of all clients associated with the access point AP01 on an 802.11a network:

```
> debug ap show stats 802.11a AP01 client all
```

Related Commands

[debug ap show stats video](#)

debug ap show stats video

To troubleshoot video messages and statistics of Cisco lightweight access points, use the **debug ap show stats video** command.

debug ap show stats video *cisco_ap* {**multicast mgid** *mgid_value* | **admission** | **bandwidth**}

Syntax Description

<i>cisco_ap</i>	Cisco lightweight access point name.
multicast mgid	Displays multicast database related information for the specified MGID of an access point.
<i>mgid_value</i>	Layer 2 MGID database number between 1 to 4095.
admission	Displays the video admission control.
bandwidth	Displays the video bandwidth.

Defaults

None.

Examples

This example shows how to troubleshoot the access point AP01's multicast group that is identified by the group's Layer 2 MGID database number:

```
> debug ap show stats video AP01 multicast mgid 50
```

This example shows how to troubleshoot the access point AP01's video bandwidth:

```
> debug ap show stats video AP01 bandwidth
```

Related Commands

[debug ap show stats](#)

debug arp

To configure Address Resolution Protocol (ARP) debug options, use the **debug arp** command.

debug arp {all | detail | events | message} {enable | disable}

Syntax Description	all	Configures debugging of all ARP logs.
	detail	Configures debugging of ARP detail messages.
	error	Configures debugging of ARP errors.
	message	Configures debugging of ARP messages.
	enable	Enables ARP debugging.
	disable	Disables ARP debugging.

Defaults None.

Examples This example shows how to enable ARP debug settings:

```
> debug arp error enable
```

This example shows how to disable ARP debug settings:

```
> debug arp error disable
```

Related Commands

show sysinfo
debug disable-all

debug bcast

To configure debugging of broadcast options, use the **debug bcast** command.

debug bcast {all | error | message | igmp | detail} {enable | disable}

Syntax Description	all	Configures debugging of all broadcast logs.
	error	Configures debugging of broadcast errors.
	message	Configures debugging of broadcast messages.
	igmp	Configures debugging of broadcast IGMP messages.
	detail	Configures debugging of broadcast detailed messages.
	enable	Enables the broadcast debugging.
	disable	Disables the broadcast debugging.

Defaults None.

Examples This example shows how to enable broadcast debug settings:

```
> debug bcast message enable
```

This example shows how to disable broadcast debug settings:

```
> 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	all	Configures debugging options for all CAC messages.
	event	Configures debugging options for CAC events.
	packet	Configures debugging options for selected CAC packets.
	enable	Enables the debugging.
	disable	Disables the debugging.

Defaults	Disabled.

Examples	This example shows how to enable debug CAC settings: <pre>> debug cac event enable > debug cac packet enable</pre>

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 call-control

To debug the SIP call control settings, use the **debug call-control** command.

debug call-control {all | event}{enable | disable}

Syntax Description

all	Configures debugging options for all SIP call control messages.
event	Configures debugging options for SIP call control events.
enable	Enables the SIP call control debugging settings.
disable	Disables the SIP call control debugging settings.

Defaults

Disabled.

Examples

This example shows how to enable debugging of all SIP call control messages:

```
> debug call-control all enable
```

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		
detail		Configures debugging for CAPWAP detail settings.
dtls-keepalive		Configures debugging for CAPWAP DTLS data keepalive packets settings.
errors		Configures debugging for CAPWAP error settings.
events		Configures debugging for CAPWAP events settings.
hexdump		Configures debugging for CAPWAP hexadecimal dump settings.
info		Configures debugging for CAPWAP info settings.
packet		Configures debugging for CAPWAP packet settings.
payload		Configures debugging for CAPWAP payload settings.
enable		Enables debugging of the CAPWAP command.
disable		Disables debugging of the CAPWAP command.

Command Default	None.

Examples	This example shows how to enable debug CAPWAP detail settings: > 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	mgmt	(Optional) Configures debugging for client authentication and association messages.
	load	(Optional) Configures debugging for payload activities, which is useful when the hybrid-REAP access point boots up in standalone mode.

Command Default	None.

Examples	This example shows how to debug hybrid-REAP client authentication and association messages: <pre>> debug capwap reap mgmt</pre>

Related Commands	clear lwapp private-config debug disable-all show capwap reap association show capwap reap status

debug client

To debug if the passive client is associated correctly with the access point and if the passive client has moved into the DHCP required state at the controller, use the **debug client** command.

debug client *mac_address*

Syntax Description

<i>mac_address</i>	MAC address of the client.

Command Default

None.

Examples

This example shows how to debug a passive client with mac address 00:0d:28:f4:c0:45:

```
> debug client 00:0d:28:f4:c0:45
```

Related Commands

[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

all	Configures debugging of all hardware crypto messages.
sessions	Configures debugging of hardware crypto sessions.
trace	Configures debugging of hardware crypto sessions.
warning	Configures debugging of hardware crypto sessions.
enable	Enables the hardware cryptographic debugging.
disable	Disables the hardware cryptographic debugging setting.

Defaults

None.

Examples

This example shows how to enable the debugging of hardware crypto sessions:

```
> debug crypto sessions enable
```

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	message	Configures debugging of DHCP error messages.
	packet	Configures debugging of DHCP packets.
	enable	Enables the DHCP debugging.
	disable	Disables the DHCP debugging.

Defaults None.

Examples This example shows how to enable DHCP debug settings:

```
> debug dhcp message enable
```

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

enable	Enables the debugging of DHCP packets on the service port.
disable	Disables the debugging of DHCP packets on the service port.

Command Default

None.

Examples

This example shows how to enable debugging of DHCP packets on a service port:

```
> debug dhcp service-port enable
```

Related Commands

[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	This command has no arguments or keywords.

Defaults	Disabled.

Examples	This example shows how to disable all debug messages: <pre>> debug disable-all</pre>

debug dot11

To configure dot11 events debug options, use the **debug dot11** command.

```
debug dot11 {all | load-balancing | management | mobile | nmosp | probe | rldp | rogue | state}
               {enable | disable}
```

Syntax Description

all	Configures debugging of all 802.11 messages.
load-balancing	Configures debugging of 802.11 load balancing events.
management	Configures debugging of 802.11 MAC management messages.
mobile	Configures debugging of 802.11 mobile events.
nmosp	Configures debugging of the 802.11 NMSP interface events.
rldp	Configures debugging of 802.11 Rogue Location Discovery.
rogue	Configures debugging of 802.11 rogue events.
state	Configures debugging of 802.11 mobile state transitions.
enable	Enables dot11 debugging.
disable	Disables dot11 debugging.

Defaults

None.

Examples

This example shows how to enable dot11 debug settings:

```
> debug dot11 state enable
> debug dot11 mobile enable
```

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 debug 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	This example shows how to debug dot11 management interface events: <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 debug 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	This example shows how to debug dot11 management messages: > debug dot11 mgmt msg

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 debug 802.11 Service Set Identifier (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	This example shows how to debug dot11 SSID management events: <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 debug the 802.11 state machine, use the **debug dot11 mgmt state-machine** command.

debug dot11 mgmt state-machine

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	This example shows how to debug dot11 state machine settings: > debug dot11 mgmt state-machine

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 debug 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	This example shows how to debug management station settings: <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

aaa	Configures debugging of 802.1X AAA interactions.
all	Configures debugging of all 802.1X messages.
events	Configures debugging of 802.1X events.
packet	Configures debugging of 802.1X mobile state transitions.
states	Configures debugging of 802.1X mobile state transitions.
enable	Enables dot1x debugging.
disable	Disables dot1x debugging.

Defaults

None.

Examples

This example shows how to enable debugging of dot1x mobile state transitions:

```
> debug dot1x states enable
```

This example shows how to disable debugging of all dot1x interactions:

```
> 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 debugging of access point groups, use the **debug group** command.

debug group {enable | disable}

Syntax Description	enable	Enables access point group debugging.
	disable	Disables access point group debugging.

Defaults None.

Examples This example shows how to enable debugging of access point groups:

```
> debug group enable
```

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

event	Configures debugging for HREAP RADIUS server events.
error	Configures debugging for HREAP RADIUS server errors.
enable	Enables debugging of hybrid-REAP RADIUS server settings.
disable	Disables debugging of hybrid-REAP RADIUS server settings.

Command Default

None.

Examples

This example shows how to enable debugging of HREAP RADIUS server events:

```
> 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

enable	Enables debugging of HREAP CCKM fast roaming settings.
disable	Disables debugging of HREAP CCKM fast roaming settings.

Command Default

None.

Examples

This example shows how to enable debugging of HREAP CCKM fast roaming events:

```
> 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

enable	Enables debugging of HREAP access point groups.
disable	Disables debugging of HREAP access point groups.

Command Default

None.

Examples

This example shows how to enable debugging of HREAP access point groups:

```
> debug hreap group 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 debugging of Layer 2 age timeout messages, use the **debug l2age** command.

debug l2age {enable | disable}

Syntax Description	enable	Enables Layer2 age debug settings.
	disable	Disables Layer2 age debug settings.

Defaults	None.

Examples	This example shows how to enable Layer2 age debug settings: <pre>> debug l2age enable</pre>

Related Commands	debug disable-all

debug lwapp console cli

To begin debugging the access point console CLI, use the **debug lwapp console cli** command from the access point console port.

debug lwapp console cli

Syntax Description This command has no arguments or keywords.

Defaults None.

Usage Guidelines This access point CLI command must be entered from the access point console port.

Examples This example shows how to begin debugging the access point console:

```
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	disable	Disables MAC debugging.
	addr	Configures MAC address debugging.
	<i>MAC</i>	MAC address.

Defaults	None.

Examples	This example shows how to configure MAC address debugging settings: <pre>> debug mac addr 00.0c.41.07.33.a6</pre>

Related Commands	debug disable-all

debug media-stream

To enable or disable media stream debugging, use the **debug media-stream** command.

debug media-stream {admission | config | errors | event | history | rrc} {enable | disable}

Syntax Description

admission	Configures debugging of media stream admission.
config	Configures debugging of media stream configuration.
errors	Configures debugging of media stream errors.
event	Configures debugging of media stream events.
history	Configures debugging of media stream history.
rrc	Configures debugging of media stream radio resource management.
enable	Enables debugging of media stream.
disable	Disables debugging of media stream.

Defaults

None.

Examples

This example shows how to enable debugging of the media stream history:

```
> debug media-stream history enable
```

Related Commands

[config media-stream multicast direct](#)
[show media-stream group summary](#)

debug memory

To enable or disable debugging of errors or events during controller memory allocation, use the **debug memory** command

debug memory {errors | events} {enable | disable}

Syntax Description	errors	Troubleshoots memory leak errors.
	events	Troubleshoots memory leak events.
	enable	Enables debugging of memory leak events.
	disable	Disables debugging of memory leak events.

Command Default	Disabled.

Examples	This example shows how to enable debugging of memory leak events: <pre>> debug memory events enable</pre>

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

all	Debugs all mesh security messages.
events	Debugs mesh security event messages.
errors	Debugs mesh security error messages.
enable	Enables debugging of mesh security error messages.
disable	Disables debugging of mesh security error messages.

Defaults

None.

Examples

This example shows how to enable debugging of mesh security error messages:

```
> debug mesh security errors enable
```

Related Commands

[config mesh security](#)
[show mesh security-stats](#)

debug mobility

To debug wireless mobility issues, use the **debug mobility** command.

```
debug mobility {{directory | handoff | multicast} {enable | disable} |  
keep-alive {enable | disable} IP_address
```

Syntax Description

directory	Starts debugging of wireless mobility error messages.
handoff	Starts debugging of wireless mobility packets.
multicast	Starts debugging of multicast mobility packets.
enable	Enables debugging of the wireless mobility feature.
disable	Disables debugging of the wireless mobility feature.
keep-alive	Starts debugging of wireless mobility keepalive messages.
<i>IP_address</i>	IP address of the wireless mobility client.

Defaults

None.

Examples

This example shows how to enable debugging of wireless mobility packets:

```
> debug mobility handoff 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 debugging of Network Access Control (NAC), use the **debug nac** command.

debug nac {events | packet} {enable | disable}

Syntax Description

events	Configures debugging of NAC events.
packet	Configures debugging of NAC packets.
enable	Enables NAC debugging.
disable	Disables NAC debugging.

Defaults

None.

Examples

This example shows how to enable NAC debug settings:

```
> debug nac events enable
```

Related Commands

[show nac statistics](#)
[show nac summary](#)
[config guest-lan nac](#)
[config wlan nac](#)

debug nmsp

To configure debugging of the Network Mobility Services Protocol (NMSP), use the **debug nmsp** command.

debug nmsp {all | connection | detail | error | event | message | packet}

Syntax Description

all	Configures debugging for all NMSP messages.
connection	Configures debugging for NMSP connection events.
detail	Configures debugging for NMSP events in detail.
error	Configures debugging for NMSP error messages.
event	Configures debugging for NMSP events.
message	Configures debugging for NMSP transmit and receive messages.
packet	Configures debugging for NMSP packet events.

Defaults

None.

Examples

This example shows how to configure debugging of NMSP connection events:

```
> debug nmsp connection
```

Related Commands

[clear nmsp statistics](#)
[debug disable-all](#)
[config nmsp notify-interval measurement](#)

debug ntp

To configure debugging of the Network Time Protocol (NTP), use the **debug ntp** command.

debug ntp {detail | low | packet} {enable | disable}

Syntax Description	detail	Configures debugging of detailed NTP messages.
	low	Configures debugging of NTP messages.
	packet	Configures debugging of NTP packets.
	enable	Enables NTP debugging.
	disable	Disables NTP debugging.

Defaults	None.

Examples	This example shows how to enable NTP debug settings: <pre>> debug ntp packet enable</pre>

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	events	Configures debugging of the policy manager events.
	state	Configures debugging of the policy manager state machine.
	enable	Enables access policy manager debugging.
	disable	Disables access policy manager debugging.

Defaults None.

Examples This example shows how to enable access policy manager debug settings:

```
> debug pem state enable
```

Related Commands debug disable-all

debug pm

To configure debugging of the security policy manager module, use the **debug pm** command.

```
debug pm {all disable | {config | hwcrypto | ikemsg | init | list | message | pki | rng | rules |
sa-export | sa-import | ssh-l2tp | ssh-appgw | ssh-engine | ssh-int | ssh-pmgr | ssh-ppp |
ssh-tcp} {enable | disable}}
```

Syntax Description

all disable	Disables all debugging in the policy manager module.
config	Configures debugging of the policy manager configuration.
hwcrypto	Configures debugging of hardware offload events.
ikemsg	Configures debugging of Internet Key Exchange (IKE) messages.
init	Configures debugging of policy manager initialization events.
list	Configures debugging of policy manager list mgmt.
message	Configures debugging of policy manager message queue events.
pki	Configures debugging of Public Key Infrastructure (PKI) related events.
rng	Configures debugging of random number generation.
rules	Configures debugging of Layer 3 policy events.
sa-export	Configures debugging of SA export (mobility).
sa-import	Configures debugging of SA import (mobility).
ssh-l2tp	Configures debugging of policy manager l2TP handling.
ssh-appgw	Configures debugging of application gateways.
ssh-engine	Configures debugging of the policy manager engine.
ssh-int	Configures debugging of the policy manager interceptor.
ssh-pmgr	Configures debugging of the policy manager.
ssh-ppp	Configures debugging of policy manager PPP handling.
ssh-tcp	Configures debugging of policy manager TCP handling.
enable	Enables the debugging.
disable	Disables the debugging.

Defaults

None.

Examples

This example shows how to configure debugging of PKI-related events:

```
> debug pm pki enable
```

Related Commands

[debug disable-all](#)

debug poe

To configure debugging of Power over Ethernet (PoE) debug options, use the **debug poe** command.

debug poe {detail | error | message} {enable | disable}

Syntax Description	detail	Configures debugging of PoE detail logs.
	error	Configures debugging of PoE error logs.
	message	Configures debugging of PoE messages.
	enable	Enables the PoE debugging.
	disable	Disables the PoE debugging.

Defaults	None.

Examples	This example shows how to enable PoE debug settings: <pre>> debug poe message enable</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

all	Configures debugging of RBC.
detail	Configures debugging of RBC detail.
errors	Configures debugging of RBC errors.
packet	Configures debugging of RBC packet trace.
enable	Enables RBC debugging.
disable	Disables RBC debugging.

Defaults

None.

Examples

This example shows how to enable RBC debug settings:

```
> debug rbc packet enable
```

Related Commands

debug disable-all

debug rfid

To configure radio-frequency identification (RFID) debug options, use the **debug rfid** command.

debug rfid {all | detail | errors | nmsp | receive} {enable | disable}

Syntax Description	all	Configures debugging of all RFID.
	detail	Configures debugging of RFID detail.
	errors	Configures debugging of RFID error messages.
	nmsp	Configures debugging of RFID Network Mobility Services Protocol (NMSP) messages.
	receive	Configures debugging of incoming RFID tag messages.
	enable	Enables RFID debugging.
	disable	Disables RFID debugging.

Defaults None.

Examples This example shows how to enable debugging of RFID error messages:

```
> debug rfid errors enable
```

Related Commands [debug disable-all](#)

debug service ap-monitor

To debug the access point monitor service, use the **debug service ap-monitor** command.

debug service ap-monitor {all | error | event | nmosp | packet} {enable | disable}

Syntax Description

all	Configures debugging of all access point status messages.
error	Configures debugging of access point monitor error events.
event	Configures debugging of access point monitor events.
nmosp	Configures debugging of access point monitor Network Mobility Services Protocol (NMSP) events.
packet	Configures debugging of access point monitor packets.
enable	Enables debugging for access point monitor service.
disable	Disables debugging for access point monitor service.

Command Default

None.

Examples

This example shows how to debug access point monitor NMSP events:

```
> debug service ap-monitor events
```

Related Commands

[debug disable-all](#)
[show nmosp status](#)

debug snmp

To configure SNMP debug options, use the **debug snmp** command.

debug snmp {agent | all | mib | trap} {enable | disable}

Syntax Description	agent	Configures debugging of the SNMP agent.
	all	Configures debugging of all SNMP messages.
	mib	Configures debugging of the SNMP MIB.
	trap	Configures debugging of SNMP traps.
	enable	Enables SNMP debugging.
	disable	Disables SNMP debugging.

Defaults None.

Examples This example shows how to enable SNMP debug settings:

```
> debug snmp trap enable
```

Related Commands debug disable-all

debug transfer

To configure transfer debug options, use the **debug transfer** command.

debug transfer {all | tftp | trace} {enable | disable}

Syntax Description

all	Configures debugging of all transfer messages.
tftp	Configures debugging of TFTP transfers.
trace	Configures debugging of transfer/upgrade.
enable	Enables transfer debugging.
disable	Disables transfer debugging.

Defaults

None.

Examples

This example shows how to enable transfer/upgrade settings:

```
> debug transfer trace enable
```

Related Commands

debug disable-all

debug voice-diag

To trace call or packet flow, use the **debug voice-diag** command.

debug voice-diag {**enable** *client_mac1* [*client_mac2*] [**verbose**] | **disable**}

Syntax Description

enable	Enables voice diagnostics for voice client(s) involved in a call.
disable	Disables voice diagnostics for voice client(s) involved in a call.
client_mac1	MAC address of a voice client.
client_mac2	(Optional) MAC address of an additional voice client.
	Note Voice diagnostics can be enabled or disabled for a maximum of two voice clients at a time.
verbose	(Optional) Enables debug information to be displayed on the console.
	Note When voice diagnostics is enabled from the WCS, the verbose option is not available.

Defaults

None.

Usage Guidelines

Follow these guidelines when you use the **debug voice-diag** command:

- When the command is entered, the validity of the client(s) is not checked.
- A few output messages of the command are sent to the WCS.
- The command expires automatically after 60 minutes.
- The command provides the details of the call flow between a pair of client MACs involved in an active call.



Note

Voice diagnostics can be enabled for a maximum of two voice clients at a time.

Examples

This example shows how to enable transfer/upgrade settings:

```
> debug voice-diag enable 00:1a:a1:92:b9:5c 00:1a:a1:92:b5:9c verbose
```

Related Commands

[show client calls](#)
[show client voice-diag](#)

debug wcp

To configure WLAN Control Protocol (WCP) debug options, use the **debug wcp** command.

debug wcp {events | packet} {enable | disable}

Syntax Description	events	Configures debugging of WCP events.
	packet	Configures debugging of WCP packets.
	enable	Enables WCP debugging settings.
	disable	Disables WCP debugging settings.

Defaults	None.

Examples	This example shows how to enable WCP debug settings: > debug wcp packet enable

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

enable	Enables debugging for WPS settings.
disable	Disables debugging for WPS settings.

Defaults

None.

Examples

This example shows how to enable WPS signature settings:

```
> debug wps sig enable
```

Related Commands

[debug disable-all](#)
[debug wps mfp](#)

debug wps mfp

To debug WPS Management Frame Protection (MFP) settings, use the **debug wps mfp** command.

debug wps mfp {**client** | **capwap** | **detail** | **report** | **mm**} {**enable** | **disable**}

Syntax Description	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	Enables debugging for WPS MFP settings.
	disable	Disables debugging for WPS MFP settings.

Defaults None.

Examples This example shows how to enable debugging of WPS MFP settings:

```
> debug wps mfp detail enable
```

Related Commands [debug disable-all](#)
[debug wps sig](#)

eping

To test the mobility Ethernet over IP (EoIP) data packet communication between two controllers, use the **eping** command.

eping *mobility_peer_IP_address*

Syntax Description

mobility_peer_IP_address 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

This example shows how to test EoIP data packets and to set the IP address of a controller that belongs to a mobility group to 172.12.35.31:

```
> 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

mobility_peer_IP_address 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

This example shows how to test mobility UDP control packet communications and to set the IP address of a controller that belongs to a mobility group to 172.12.35.31:

```
> mping 172.12.35.31
```

Related Commands

eping
config logging buffered debugging
show logging
debug mobility handoff enable