



Cisco Wireless LAN Controller Commands

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

This document covers the commands available in the Cisco CLI release 5.0. The controllers currently covered include:

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

This chapter contains the following sections:

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

Using the ? command

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

?

command name ?

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

Examples

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

```
> ?
```

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

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

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

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

```
> transfer download datatype ?
```

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

Using the Help Command

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

help

Examples

```
> help
```

```
HELP:
```

```
Special keys:
```

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

Show Commands for Viewing Configuration

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

Show 802.11x Commands

To view **show** commands for the 802.11a, 802.11b, or other supported 802.11 network, use the **show 802.11x** commands.

show 802.11a

To display basic 802.11a options and settings, use the **show 802.11a** command.

show 802.11a

Syntax Description	show	Displays configurations.
	802.11a	802.11a configurations.

Defaults None.

Examples

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

```

MCS 15..... Supported
802.11n Status:
  A-MPDU Tx ..... Enabled
    Priority 0..... Enabled
    Priority 1..... Enabled
    Priority 2..... Enabled
    Priority 3..... Enabled
    Priority 4..... Enabled
    Priority 5..... Disabled
    Priority 6..... Disabled
    Priority 7..... Enabled
  A-MSDU Tx ..... Enabled
  Rifs Tx ..... Enabled
  Guard Interval ..... Short
  Beacon Interval..... 100
  CF Pollable mandatory..... Disabled
  CF Poll Request mandatory..... Disabled
  CFP Period..... 4
  CFP Maximum Duration..... 60
  Default Channel..... 36
  Default Tx Power Level..... 1
  DTPC Status..... Enabled
  Fragmentation Threshold..... 2346
  Long Retry Limit..... 4
  Maximum Rx Life Time..... 512
  Max Tx MSDU Life Time..... 512
  Medium Occupancy Limit..... 100
  Pico-Cell Status..... Disabled
  Pico-Cell-V2 Status..... Disabled
  RTS Threshold..... 2347
  Short Retry Limit..... 7
  TI Threshold..... -50
  Traffic Stream Metrics Status..... Disabled
  Expedited BW Request Status..... Disabled
  EDCA profile type..... default-wmm
  Voice MAC optimization status..... Disabled
  Call Admission Control (CAC) configuration
    Voice AC - Admission control (ACM)..... Disabled
      Voice max RF bandwidth..... 75
      Voice reserved roaming bandwidth..... 6
      Voice load-based CAC mode..... Disabled
      Voice tspec inactivity timeout..... Disabled
      Video AC - Admission control (ACM)..... Disabled
      Voice Stream-Size..... 84000
      Voice Max-Streams..... 2
      Video max RF bandwidth..... Infinite
      Video reserved roaming bandwidth..... 0

```

Related Commands**show 802.11b****show advanced 802.11a summary**

show 802.11a l2roam

To display 802.11a Layer 2 client roaming information, use the **show 802.11a l2roam** command.

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

Syntax Description

show	Displays configurations.
802.11a	802.11a configurations.
l2roam	Layer 2 client roaming configurations.
rf-param	Radio frequency parameters.
statistics	Layer 2 client roaming statistics.
<i>mac_address</i>	The MAC address of the client.

Defaults

None.

Examples

```
> show 802.11a l2roam rf-param
```

```
L2Roam 802.11a RF Parameters.....
  Config Mode..... Default
  Minimum RSSI..... -85
  Roam Hysteresis..... 2
  Scan Threshold..... -72
  Transition time..... 5
```

Related Commands

show 802.11b l2roam

config { 802.11a | 802.11b } l2roam rf-params

show 802.11b

To display basic 802.11b/g options and settings, use the **show 802.11b** command.

show 802.11b

Syntax Description	show	Displays configurations.
	802.11b	802.11b/g configurations.

Defaults	None.

Examples

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

```

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

```

Related Commands**show 802.11a****show advanced 802.11b summary**

show 802.11b l2roam

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

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

Syntax Description		
show		Displays configurations.
802.11b		802.11b/g configurations.
l2roam		Layer 2 client roaming configurations.
rf-param		Radio frequency parameters.
statistics		Layer 2 client roaming statistics.
<i>mac_address</i>		The MAC address of the client.

Defaults None.

Examples

```
> show 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

show 802.11a l2roam

config {802.11a | 802.11b} l2roam rf-params

show 802.11h

To display basic 802.11h options and settings, use the **show 802.11h** command.

show 802.11h

Syntax Description	show	Displays configurations.
	802.11h	802.11h configurations.

Defaults	None.

Examples	<pre>> show 802.11h 802.11h powerconstraint : 0 802.11h channelswitch : Disable 802.11h channelswitch mode : 0</pre>

Related Commands	show 802.11a show 802.11b config 802.11h

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	This command has no defaults.

Examples	<pre>> show aaa auth Management authentication server order: 1..... local 2..... tacacs</pre>

Related Commands	config aaa auth

show acl

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

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

Syntax Description

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

Defaults

None.

Examples

> **show acl summary**

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

> **show acl detailed** *acl_name*

```

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

DenyCounter : 0



Note

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

Related Commands

clear acl counters
config acl counter
config interface acl

show acl cpu

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

show acl cpu

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

Command Default	None

Examples

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

Related Commands	config acl cpu

Show Advanced 802.11a Commands

Use the **show advanced 802.11a** commands to show advanced 802.11a parameters.

show advanced 802.11a channel

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

show advanced 802.11a channel

Syntax Description

show	Displays configurations.
advanced	Advanced parameters.
802.11a	802.11a network.
channel	Channel status.

Defaults

None.

Examples

> **show advanced 802.11a channel**

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

Related Commands

config 802.11a channel

show advanced 802.11a coverage

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

show advanced 802.11a coverage

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	802.11a	802.11a network.
	coverage	Coverage hole detection.

Defaults None.

Examples

```
> show advanced 802.11a coverage

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

Related Commands

- [config advanced 802.11a coverage](#)
- [config advanced 802.11a coverage exception global](#)
- [config advanced 802.11a coverage fail-rate](#)
- [config advanced 802.11a coverage level global](#)
- [config advanced 802.11a coverage packet-count](#)
- [config advanced 802.11a coverage rssi-threshold](#)

show advanced 802.11a group

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

show advanced 802.11a group

Syntax Description

show	Displays configurations.
advanced	Advanced parameters.
802.11a	802.11a network.
group	RF grouping values.

Defaults

None.

Examples

```
> show advanced 802.11a group
```

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

Related Commands

config advanced 802.11a group-mode

show advanced 802.11a logging

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

show advanced 802.11a logging

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	802.11a	802.11a network.
	logging	RF event and performance logging.

Defaults	None.

Examples

```
> show advanced 802.11a 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 802.11a logging channel, config advanced 802.11a logging coverage, config advanced 802.11a logging foreign, config advanced 802.11a logging load, config advanced 802.11a logging noise, config advanced 802.11a logging performance, config advanced 802.11a logging power

show advanced 802.11a monitor

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

show advanced 802.11a monitor

Syntax Description

show	Displays configurations.
advanced	Advanced parameters.
802.11a	802.11a network.
monitor	Cisco radio monitoring values.

Defaults

None.

Examples

```
> show advanced 802.11a monitor
```

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

Related Commands

config advanced 802.11a monitor coverage
config advanced 802.11a monitor load
config advanced 802.11a monitor noise
config advanced 802.11a monitor signal

show advanced 802.11a profile

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

show advanced 802.11a profile {**global** | *Cisco_AP*}

Syntax Description		
show		Displays configurations.
advanced		Advanced parameters.
802.11a		802.11a network.
profile		Cisco radio performance profile.
global		All Cisco lightweight access points.
<i>Cisco_AP</i>		The name of a specific Cisco lightweight access point.

Defaults None.

Examples

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

```
Default 802.11a AP performance profiles
 802.11a Global Interference threshold..... 10%
 802.11a Global noise threshold..... -70 dBm
 802.11a Global RF utilization threshold..... 80%
 802.11a Global throughput threshold..... 1000000 bps
 802.11a Global clients threshold..... 12 clients
```

```
> 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 802.11b profile clients**
- config advanced 802.11b profile customize**
- config advanced 802.11b profile foreign**
- config advanced 802.11b profile noise,**
- config advanced 802.11b profile throughput**
- config advanced 802.11b profile utilization**

show advanced 802.11a receiver

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

show advanced 802.11a receiver

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	802.11a	802.11a network.
	receiver	Receiver.

Defaults None.

Examples

> **show advanced 802.11a receiver**

```
802.11a Advanced 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
RxAabort  : Raw Power Drop Status..... Disabled
RxAabort  : Raw Power Drop Threshold..... 10
RxAabort  : Low RSSI Status..... Disabled
RxAabort  : Low RSSI Threshold..... 0
RxAabort  : Wrong BSSID Status..... Disabled
RxAabort  : Wrong BSSID Data Only Status..... Disabled
```

Related Commands

- config advanced 802.11a monitor coverage**
- config advanced 802.11a monitor load**
- config advanced 802.11a monitor noise**
- config advanced 802.11a monitor signal**

show advanced 802.11a summary

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

show advanced 802.11a summary

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	802.11a	802.11a network.
	summary	Cisco lightweight access point name, channel, and transmit level summary.

Defaults None.

Examples

```
> show advanced 802.11a summary
```

AP Name	Channel	TxPower Level
AP03	36*	1*
AP02	52	5*
AP01	64	5



Note

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

Related Commands **show advanced 802.11b summary**

show advanced 802.11a txpower

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

show advanced 802.11a txpower

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	802.11a	802.11a network.
	txpower	Transmit power.

Defaults None.

Examples

```
> show advanced 802.11a 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 802.11a txpower-update, config 802.11a txPower

Show Advanced 802.11b Commands

Use the **show advanced 802.11b** commands to show advanced 802.11b parameters.

show advanced 802.11b channel

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

show advanced 802.11b channel

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	802.11b	802.11b/g network.
	channel	Channel status.

Defaults None.

Examples

> **show advanced 802.11b channel**

```
Automatic Channel Assignment
Channel Assignment Mode..... ONCE
Channel Update Interval..... 600 seconds
Anchor time (Hour of the day)..... 14
Channel Update Count..... 0
Channel Update Contribution..... S.IU
Channel Assignment Leader..... 00:0b:85:40:90:c0
Last Run..... 10 seconds ago

DCA Sensitivity Level: ..... MEDIUM (15 dB)
Channel Energy Levels
  Minimum..... unknown
  Average..... unknown
  Maximum..... unknown
Channel Dwell Times
  Minimum..... 0 days, 01 h 44 m 25 s
  Average..... 0 days, 01 h 45 m 00 s
  Maximum..... 0 days, 01 h 45 m 35 s
Auto-RF Allowed Channel List..... 1,6,11
Auto-RF Unused Channel List..... 2,3,4,5,7,8,9,10
```

Related Commands **config 802.11b channel**

show advanced 802.11b coverage

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

show advanced 802.11b coverage

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	802.11b	802.11a network.
	coverage	Coverage hole detection.

Defaults None.

Examples

> **show advanced 802.11b coverage**

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

Related Commands

[config advanced 802.11b coverage](#)
[config advanced 802.11b coverage exception global](#)
[config advanced 802.11b coverage fail-rate](#)
[config advanced 802.11b coverage level global](#)
[config advanced 802.11b coverage packet-count](#)
[config advanced 802.11b coverage rssi-threshold](#)

show advanced 802.11b group

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

show advanced 802.11b group

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	802.11b	802.11b/g network.
	group	RF grouping values.

Defaults None.

Examples

```
> show advanced 802.11b group
```

```
Radio RF Grouping
 802.11b Group Mode..... AUTO
 802.11b Group Update Interval..... 600 seconds
 802.11b Group Leader..... xx:xx:xx:xx:xx:xx
   802.11b Group Member..... xx:xx:xx:xx:xx:xx
 802.11b Last Run..... 511 seconds ago
```

Related Commands **config advanced 802.11b group-mode**

show advanced 802.11b logging

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

show advanced 802.11b logging

Syntax Description

show	Displays configurations.
advanced	Advanced parameters.
802.11b	802.11b network.
logging	RF event and performance logging.

Defaults

None.

Examples

> **show advanced 802.11b logging**

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

Related Commands

config advanced 802.11b logging channel
config advanced 802.11b logging coverage
config advanced 802.11b logging foreign
config advanced 802.11b logging load
config advanced 802.11b logging noise
config advanced 802.11b logging performance
config advanced 802.11b logging power

show advanced 802.11b monitor

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

show advanced 802.11b monitor

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	802.11b	802.11b/g network.
	monitor	Cisco radio monitoring values.

Defaults None.

Examples

```
> show advanced 802.11b monitor

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

Related Commands

- config advanced 802.11b monitor coverage**
- config advanced 802.11b monitor load**
- config advanced 802.11b monitor noise**
- config advanced 802.11b monitor signal**

show advanced 802.11b profile

To display the advanced 802.11b/g Cisco radio performance profiles, use the **show advanced 802.11b profile** command.

show advanced 802.11b profile {global | Cisco_AP}

Syntax Description

show	Displays configurations.
advanced	Advanced parameters.
802.11b	802.11b/g network.
profile	Cisco lightweight access point performance profile.
global	All Cisco lightweight access points.
<i>Cisco_AP</i>	The name of Cisco lightweight access point.

Defaults

None.

Examples

```
> show advanced 802.11b profile global
```

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

```
> show advanced 802.11b profile AP1
```

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

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

Related Commands

config advanced 802.11b profile clients
config advanced 802.11b profile customize
config advanced 802.11b profile foreign
config advanced 802.11b profile noise
config advanced 802.11b profile throughput
config advanced 802.11b profile utilization

show advanced 802.11b receiver

To display the advanced 802.11b/g default Cisco radio receiver parameters, use the **show advanced 802.11b receiver** command.

show advanced 802.11b receiver

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	802.11b	802.11b/g network.
	receiver	Cisco radio receiver values.

Defaults None.

Examples

> **show advanced 802.11b receiver**

```
Default 802.11b Receiver Settings
RxStart    : Signal Threshold..... 15
RxStart    : Signal Jump Threshold..... 5
RxStart    : Preamble Power Threshold..... 2
RxRestart  : Signal Jump Status..... Enabled
RxRestart  : Signal Jump Threshold..... 10
TxStomp    : Low RSS Status. .... Disabled
TxStomp    : Low RSSI Threshold..... 37
TxStomp    : Wrong BSSID Status..... Disabled
TxStomp    : Wrong BSSID Data Only Status... Disabled
RxAbort    : Raw Power Drop Status..... Disabled
RxAbort    : Raw Power Drop Threshold..... 0
RxAbort    : Low RSSI Status..... Enabled
RxAbort    : Low RSSI Threshold..... 0
RxAbort    : Wrong BSSID Status..... Disabled
RxAbort    : Wrong BSSID Data Only Status... Disabled
```

Related Commands

- config advanced 802.11b monitor coverage**
- config advanced 802.11b monitor load**
- config advanced 802.11b monitor noise**
- config advanced 802.11b monitor signal**

show advanced 802.11b summary

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

show advanced 802.11b summary

Syntax Description

show	Displays configurations.
advanced	Advanced parameters.
802.11b	802.11b/g network.
summary	Cisco lightweight access point name, channel, and transmit level summary.

Defaults

None.

Examples

```
> show advanced 802.11b summary
```

AP name	Channel	Txpower Level
-----	-----	-----
AP1	11 *	1 *
AP2	10 *	4
AP3	6 *	2



Note

Asterisks next to channel numbers or power levels indicate that they are being controlled by the global algorithm settings.

Related Commands

show advanced 802.11a summary

show advanced 802.11b txpower

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

show advanced 802.11b txpower

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	802.11b	802.11b/g network.
	txpower	Transmit power.

Defaults None.

Examples

> **show advanced 802.11b txpower**

```
Automatic Transmit Power Assignment
Transmit Power Assignment Mode..... AUTO
Transmit Power Update Interval..... 600 seconds
Transmit Power Threshold..... -65 dBm
Transmit Power Neighbor Count..... 3 APs
Transmit Power Update Contribution..... SNI.
Transmit Power Assignment Leader..... xx:xx:xx:xx:xx:xx
Last Run..... 427 seconds ago
```

Related Commands **config 802.11b txPower**

show advanced backup-controller

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

show advanced backup-controller

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	backup-controller	Advanced backup controller list.

Defaults

None.

Examples

```
> show advanced backup-controller

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

Related Commands

config advanced backup-controller primary, config advanced backup-controller secondary

Other Show Advanced Commands

Use these **show advanced** commands to show other advanced parameters.

show advanced client-handoff

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

show advanced client-handoff

Syntax	Description
show	Displays configurations.
advanced	Advanced parameters.
client-handoff	Advanced client handoff count.

Defaults None.

Examples

```
> show advanced client-handoff

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

Related Commands

- config advanced timers auth-timeout**
- config advanced timers rogue-ap**

show advanced eap

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

show advanced eap

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	eap	Advanced client handoff count.

Defaults None.

Examples

```
> show advanced eap

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

Related Commands None.

show advanced max-1x-sessions

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

show advanced max-1x-sessions

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	max-1x-sessions	Maximum number of simultaneous 802.1x sessions allowed per access point.

Defaults	None.

Examples	<pre>> show advanced max-1x-sessions Max 802.1x session per AP at a given time..... 0</pre>

Related Commands	None.

show advanced probe-limit

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-limit** command.

show advanced probe-limit

Syntax Description

show	Displays configurations.
advanced	Advanced parameters.
probe-limit	Number of probes sent to the WLAN controller per access point per client and the probe interval in milliseconds.

Defaults

None.

Examples

```
> show advanced probe-limit
```

```
Probes sent to switch per AP slot per client.... 2
Probe interval in msec..... 500
```

Related Commands

None.

show advanced rate

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

show advanced rate

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	rate	Control path rate limiting enabled or disabled.

Defaults None.

Examples

```
> show advanced rate
Control Path Rate Limiting..... Disabled
```

Related Commands None.

show advanced send-disassoc-on-handoff

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

show advanced send-disassoc-on-handoff

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	send-disassoc-on-handoff	WLAN controller disassociates clients after a handoff enabled or disabled.

Defaults	None.

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

Related Commands	None.

show advanced statistics

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

show advanced statistics

Syntax Description

show	Displays configurations.
advanced	Advanced parameters.
statistics	Show Cisco Wireless LAN controller port statistics state.

Defaults

None.

Examples

```
> show advanced statistics  
Switch port statistics..... Enabled
```

Related Commands

config advanced timers auth-timeout
config advanced timers rogue-ap

show advanced timers

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

show advanced timers

Syntax Description

show	Displays configurations.
advanced	Advanced parameters.
timers	Advanced system timers.

Defaults

Shown below in examples.

Examples

```
> show advanced timers
```

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

Related Commands

config advanced timers auth-timeout
config advanced timers rogue-ap

Show AP Commands

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

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 {802.11a | 802.11b} Cisco_AP

Syntax	Description
show	Displays configurations.
ap auto-rf	Cisco radio.
{802.11a 802.11b}	802.11a or 802.11b/g setting.
Cisco_AP	Cisco lightweight access point name.

Defaults None.

Examples

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

```

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

```

```

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

```

Related Commands**config 802.11a antenna****config 802.11b antenna****config cell**

show ap ccx rm

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

show ap ccxrm *ap_name* status

Syntax Description

<i>ap_name</i>	Specified the access point name.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

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

A Radio

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

G Radio

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

Related Commands

show client ccx

show ap cdp neighbors detail

This command is used to display information regarding the access point's CDP neighbors.

show ap cdp neighbors detail [**all** | *ap_name*]

Syntax Description	all	Displays the CDP neighbors for all the access points.
	<i>ap_name</i>	Displays the CDP neighbors for the specified access point.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> show ap cdp neighbors all
```

```
AP Name:A10-1130
AP IP address:10.00.231.100
-----
Device ID: Switch
Entry address(es): 10.00.231.2
Platform: cisco WS-C3750-24P, Capabilities: Router Switch IGMP
Interface: enet, Port ID (outgoing port): FastEthernet1/0/23 Holdtime: 180 sec

Version:
Cisco Internetwork Operating System Software IOS (tm) C3750 Software (C3750-I9- M),
Version 12.2(20)SE4, RELEASE SOFTWARE (fc1) Copyright (c) 1986-2005 by Cisco Systems,
Inc. Compiled Sun 09-Jan-05 00:09 by antonino

advertisement version: 2
```

Related Commands None.

show ap config

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

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

Syntax	Description
802.11a	Displays the 802.11a radio settings.
802.11b	Displays the 802.11b/g radio settings.
general	Displays general access point settings.
<i>Cisco_AP</i>	Specifies the lightweight access point name.

Defaults None.

Examples

> **show ap config 802.11a AP02**

```

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

Attributes for Slot 0
  Radio Type..... RADIO_TYPE_80211a
  Administrative State ..... ADMIN_ENABLED
  Operation State ..... UP
  WLAN Override..... Disabled
  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
Antenna Type..... INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBm units).... 11
AntennaMode..... ANTENNA_OMNI

Performance Profile Parameters
Configuration ..... AUTOMATIC
Interference threshold..... 10%
Noise threshold..... -70 dBm
RF utilization threshold..... 80%
Data-rate threshold..... 1000000 bps
Client threshold..... 12 clients
Coverage SNR threshold..... 16 dB

```

```

Coverage exception level..... 25%
Client minimum exception level..... 3 clients
Rogue Containment Information
Containment Count..... 0

```

> **show ap config 802.11b AP02**

```

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

```

Attributes for Slot 1

```

Radio Type..... RADIO_TYPE_80211g
Administrative State ..... ADMIN_ENABLED
Operation State ..... UP
WLAN Override ..... Disabled
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
Antenna Type..... INTERNAL_ANTENNA
Internal Antenna Gain (in5 dBm units)..... 11
Diversity..... DIVERSITY_ENABLED

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

> show ap config general cisco-ap

Cisco AP Identifier..... 1
Cisco AP Name..... cisco-ap
Country code..... Multiple Countries:US,CA
Regulatory Domain allowed by Country..... 802.11bg:-AB 802.11a:-AB
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..... Static IP assigned
IP Address..... 10.10.10.21

```



```

IP NetMask..... 255.255.255.0
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
Remote AP Debug ..... Disabled
S/W Version ..... 5.1.0.0
Boot Version ..... 12.4.10.0
Mini IOS Version ..... 0.0.0.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Enabled
PoE Power Injector MAC Addr..... Disabled
Power Type/Mode..... PoE/Low Power (degraded mode)
Number Of Slots..... 2
AP Model..... AIR-LAP1252AG-A-K9
IOS Version..... 12.4(10:0)
Reset Button..... Enabled
AP Serial Number..... serial_number
AP Certificate Type..... Manufacture Installed
Management Frame Protection Validation..... Enabled (Global MFP Disabled)
AP User Mode..... CUSTOMIZED
AP User Name..... maria
AP Dot1x User Mode..... Not Configured
AP Dot1x User Name..... Not Configured
Cisco AP system logging host..... 255.255.255.255
AP Up Time..... 4 days, 06 h 17 m 22 s
AP LWAPP Up Time..... 4 days, 06 h 15 m 00 s
Join Date and Time..... Mon Mar 3 06:19:47 2008

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

```

Related Commands**config 802.11a antenna****config 802.11b antenna****config 802.11a enable****config 802.11b enable**

show ap config global

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

show ap config global

Syntax Description	show ap config	Displays Cisco radio configurations.
	global	Targeted towards all access points joined to the controller.

Defaults	None.

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

Related Commands	show ap config general

show ap core-dump

To display the memory core dump setting 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

> show ap core-dump AP02

Related Commands

config ap core-dump

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	This command has no defaults.

Examples	> show ap crash-file

Related Commands	config ap crash-file

show ap eventlog

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

show ap eventlog *ap_name*

Syntax Description	<i>ap_name</i>	Displays the event log for the specified access point.

Defaults	None

Command History	Release	Modification
	5.1	This command was introduced.

Examples

```
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: %LWAPP-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 Dot11Radiol, 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: %LWAPP-3-CLIENTEVENTLOG: Did not get vendor specific options from
DHCP.
...
```

Related Commands	clear ap-eventlog

show ap inventory

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

show ap inventory *ap_name*

Syntax Description

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

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> show ap inventory test101
```

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

Related Commands

None.

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	show	Displays configurations.
	ap	All Cisco lightweight access points.
	join stats detailed	Join-related statistics collected for a specific access point.
	ap_mac	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.

Defaults None.

Examples

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

```
Discovery phase statistics
- Discovery requests received..... 2
- Successful discovery responses sent..... 2
- Unsuccessful discovery request processing..... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt..... Aug 21 12:50:23:335
- Time at last unsuccessful discovery attempt..... Not applicable

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

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

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

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

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

Related Commands

- show ap join stats summary all
- show ap join stats summary

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*



Note To obtain the MAC address of the 802.11 radio interface, enter the **show interfaces Dot11Radio 0** command on the access point.

Syntax Description

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

Defaults

None.

Examples

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

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

Related Commands

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

Defaults	None.

Examples	<pre>> show ap join stats summary all Number of APs..... 3 00:0b:85:1b:7c:b0..... Joined 00:12:44:bb:25:d0..... Joined 00:13:19:31:9c:e0..... Not joined</pre>

Related Commands	show ap join stats summary

show ap stats

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

show ap stats {802.11a | 802.11b | wlan} Cisco_AP

Syntax	Description
show	Displays configurations.
ap stats	Cisco radio.
802.11a	802.11a statistics.
802.11b	802.11b/g statistics.
wlan	WLAN statistics.
<i>Cisco_AP</i>	Cisco lightweight access point name.

Defaults None.

Examples

> **show ap stats 802.11b AP02**

```

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

```

Related Commands

- config ap enable**
- show ap summary**

show ap summary

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

show ap summary

Syntax Description

show	Displays configurations.
ap	All Cisco lightweight access points.
summary	Summary of all Cisco lightweight access points.

Defaults

None.

Examples

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

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

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

Related Commands

config ap enable
config ap priority
config network ap-priority
show advanced 802.11a summary
show advanced 802.11b summary

show ap wlan

To display whether or not a Cisco Wireless LAN controller radio is in wireless LAN override mode (as described in the related product guide), use the **show ap wlan** command.

show ap wlan {802.11a | 802.11b} Cisco_AP

Syntax Description

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

Defaults

None.

Examples

```
> show ap wlan 802.11a AP01
```

```
AP has following wlan Id's configured as override wlanId
Wlan Id:..... 3
```

```
> show ap wlan 802.11a AP15
```

```
Cisco AP is not in override mode.
```

Related Commands

show ap summary
config ap wlan enable

show arp switch

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

show arp switch

Syntax Description

show	Displays configurations.
arp	arp MAC addresses, IP Addresses, and port types.
switch	Cisco Wireless LAN controller parameters.

Defaults

None.

Examples

> **show arp switch**

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

Related Commands

debug arp

show auth-list

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

show auth-list

Syntax Description	show	Displays configurations.
	auth-list	Displays access point authorization list.

Defaults None.

Examples

```
> 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 **config auth-list**

show boot

Each Cisco Wireless LAN controller retains one primary and one backup operating system software load in non-volatile RAM. This allows operators to have the Cisco Wireless LAN controllers boot off the primary load (default), or revert to the backup load when desired. To display the primary and backup software build numbers with an indication of which is active, use the **show boot** command.

show boot

Syntax Description	show	Displays configurations.
	boot	Software bootable versions.

Defaults	None.

Examples	<pre>> show boot Primary Boot Image..... 3.2.13.0 (active) Backup Boot Image..... 3.2.15.0</pre>

Related Commands	config exclusionlist add config exclusionlist delete config exclusionlist description show client

Show Certificate Commands

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

show certificate compatibility

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

show certificate compatibility

Syntax Description	show	Displays configurations.
	certificate	All certificates.
	compatibility	Compatibility of certificates.

Defaults	None.

Examples	<pre>> show certificate compatibility Certificate compatibility mode:..... off</pre>

Related Commands	show certificate summary

show certificate summary

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

show certificate summary

Syntax Description	show	Displays configurations.
	certificate	All certificates.
	summary	Synopsis of all certificates.

Defaults	None.

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

Related Commands	show certificate compatibility

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.



Note

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).

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

Syntax Description

show	Displays configurations.
client ap	Cisco radio.
802.11a	802.11a clients.
802.11b	802.11b/g clients.
<i>Cisco_AP</i>	Cisco lightweight access point name.

Defaults

None.

Examples

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

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

Related Commands

show client detail
show client summary
show client username
show exclusionlist

show client ccx client-capability

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



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

show client ccx client-capability *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

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

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

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

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

Related Commands

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

show client ccx frame-data

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

show client ccx frame-data *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

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

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

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

```

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

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

```

Related Commands

show client ccx last-response-status

show client ccx last-response-status

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

show client ccx last-response-status *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

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

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

Related Commands

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

show client ccx last-test-status

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

show client ccx last-test-status *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> show client ccx last-test-status
Test Type ..... Gateway Ping Test
Test Status ..... Pending/Success/Timeout
Dialog Token ..... 15
Timeout ..... 15000 ms
Request Time ..... 1329 seconds since system boot
```

Related Commands

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

show client ccx log-response

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

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

Syntax Description	roam	Displays CCX client roaming log response.
	rsna	Displays CCX client RSNA log response.
	syslog	Displays CCX client system log response.
	<i>client_mac_address</i>	Displays the inventory for the specified access point.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

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

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

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

```

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

```

```

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

```

```

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

```

Related Commands

config client ccx log-request

show client ccx manufacturer-info

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

show client ccx manufacturer-info *client_mac_address*

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

Defaults	This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples	<pre> > 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 </pre>

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

show client ccx operating-parameters

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

show client ccx operating-parameters *client_mac_address*

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

Defaults	This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples	<pre>> 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</pre>

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 manufacturer-info
show client ccx client-capability
config client ccx stats-request
show client ccx stats-report

show client ccx profiles

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

show client ccx profiles *client_mac_address*

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

Defaults	This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples

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

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

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

Radio Type..... ERP(802.11g)
  Preamble Type..... Long preamble
  CCA Method..... Energy Detect + Carrier
Detect/Correlation
  Data Retries..... 6
  Fragment Threshold..... 2342
```

```

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

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

```

Related Commands

```

config client ccx get-operating-parameters
config client ccx get-manufacturer-info
config client ccx get-client-capability
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

```

show client ccx results

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

show client ccx results *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

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

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

Related Commands

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

show client ccx rm

This command is used to display CCX client information.

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

Syntax Description		
<i>client_MAC</i>		Specifies the client MAC address.
status		Displays client ccx radio management status information.
report		Displays client ccx radio management report.
chan-load		Displays radio management channel load reports.
noise-hist		Displays radio management noise histogram reports.
beacon		Displays radio management beacon load reports.
frame		Displays radio management frame reports.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

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

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

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

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

```

9 13
10 222
11 75

```

> **show client ccx rm 00:40:96:15:21:ac report noise-hist**

```

Noise Histogram Report
Client Mac Address..... 00:40:96:15:21:ac
Timestamp..... 4294967295
Incapable Flag..... Off
Refused Flag..... Off
Chan RPI0 RPI1 RPI2 RPI3 RPI4 RPI5 RPI6 RPI7

```

> **show client ccx rm 00:40:96:ae:53:bc report beacon**

```

Beacon Report
Client Mac Address..... 00:40:96:ae:53:bc
Timestamp..... 788853242
Incapable Flag..... On
Refused Flag..... On

```

```

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

```

```

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

```

> **show client ccx rm 00:40:96:ae:53:bc report frame**

```

Frame Report
Client Mac Address..... 00:40:96:ae:53:bc
Timestamp..... 789140437
Incapable Flag..... On
Refused Flag..... On
Chan Tx Address Bssid RcxSigPwr Frame Count
-----

```

Related Commands None.

show client ccx stats-report

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

show client ccx stats-report *client_mac_address*

Syntax Description

<i>client_mac_address</i>	Displays the MAC address for the specified client device.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

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

Measurement duration = 1

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

Related Commands

config client ccx stats-request

show client detail

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



Note

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).

show client detail *mac_address*

Syntax Description

show	Displays configurations.
client	802.11a or 802.11b/g client.
detail	Connectivity information.
<i>mac_address</i>	MAC address of the specific client.

Defaults

None.

Examples

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

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

```
Radio Signal Strength Indicator..... Unavailable
Signal to Noise Ratio..... Unavailable
...
```

Related Commands

- show client ap**
- show client summary**
- show client username**
- show exclusionlist**

show client location-calibration summary

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

show client location-calibration summary

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> show client location-calibration summary

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

Related Commands None.

show client report

To display detail client information, use the **show client detail** command.

show client detail

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples	<pre>> show client detail 00:14:6c:0a:57:77 Client MAC Address..... 00:14:6c:0a:57:77 Client Username N/A AP MAC Address..... 00:0b:85:0e:19:a0 Client State..... Diagnostics Wireless LAN Id..... 1 BSSID..... 00:0b:85:0e:19:a0 Channel..... 40 IP Address..... 1.100.150.53 Association Id..... 1 Authentication Algorithm..... Open System Reason Code..... 0 Status Code..... 0 Session Timeout..... 1800 Client CCX version..... CCXv5 Re-Authentication Timeout..... 1800 QoS Level..... Silver</pre>

Related Commands	None.

show client summary

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



Note

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).

show client summary

Syntax Description

show	Displays configurations.
client	802.11a or 802.11b/g client.
summary	All attached clients.

Defaults

None.

Examples

```
> show client summary
```

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

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

None.

show client summary guest-lan

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

show client summary guest-lan

Syntax Description	show	Displays configurations.
	client	802.11a or 802.11b/g client.
	summary	All attached clients.
	guest-LAN	Indicates the active wired guest LAN.

Defaults None.

Examples

```
> show client summary
```

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

show client username

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

show client username *username*

Syntax Description

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

Defaults

None.

Examples

```
> show client username IT_007
```

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

Related Commands

show client ap
show client detail
show client summary

show country

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

show country

This command has no arguments or keywords.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> show country
```

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

Related Commands

config country
display country supported
show country channels

show country 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 This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> 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 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
- display country supported
- show country

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 This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

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

```

LT - Lithuania..... 802.11a / 802.11b / 802.11g
LU - Luxembourg..... 802.11a / 802.11b / 802.11g
LV - Latvia..... 802.11a / 802.11b / 802.11g
MC - Monaco..... 802.11a / 802.11b / 802.11g
MT - Malta..... 802.11a / 802.11b / 802.11g
MX - Mexico..... 802.11a / 802.11b / 802.11g
MY - Malaysia..... 802.11a / 802.11b / 802.11g
NL - Netherlands..... 802.11a / 802.11b / 802.11g
NZ - New Zealand..... 802.11a / 802.11b / 802.11g
NO - Norway..... 802.11a / 802.11b / 802.11g
PA - Panama..... 802.11b / 802.11g
PE - Peru..... 802.11b / 802.11g
PH - Philippines..... 802.11a / 802.11b / 802.11g
PL - Poland..... 802.11a / 802.11b / 802.11g
PT - Portugal..... 802.11a / 802.11b / 802.11g
RU - Russian Federation..... 802.11a / 802.11b / 802.11g
RO - Romania..... 802.11a / 802.11b / 802.11g
SA - Saudi Arabia..... 802.11a / 802.11b / 802.11g
SE - Sweden..... 802.11a / 802.11b / 802.11g
SG - Singapore..... 802.11a / 802.11b / 802.11g
SI - Slovenia..... 802.11a / 802.11b / 802.11g
SK - Slovak Republic..... 802.11a / 802.11b / 802.11g
TH - Thailand..... 802.11b / 802.11g
TR - Turkey..... 802.11b / 802.11g
TW - Taiwan..... 802.11a / 802.11b / 802.11g
UA - Ukraine..... 802.11a / 802.11b / 802.11g
US - United States..... 802.11a / 802.11b / 802.11g
USL - United States (Legacy)..... 802.11a / 802.11b / 802.11g
USX - United States (US + chan165)..... 802.11a / 802.11b / 802.11g
VE - Venezuela..... 802.11b / 802.11g
ZA - South Africa..... 802.11a / 802.11b / 802.11g

```

Related Commands

config country
display country channels
show country

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

Related Commands	show sysinfo

show custom-web

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

show custom-web

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	<pre>> 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</pre>

Related Commands	config custom-web

show database summary

To display the maximum number of entries in the database, use the **show database summary** command.

show database summary

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples	<pre>> show database summary Current Max database entries..... 512 Max database entries on next reboot..... 512</pre>

Related Commands	config database size

show debug

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

show debug

Syntax Description	show	Displays configurations.
	debug	MAC address debugging.

Defaults	None.

Examples	> show debug
	MAC debugging..... disabled
	Debug Flags Enabled:
	arp error enabled.
	bcast error enabled.

Related Commands	debug mac

show dhcp

Use the **show dhcp** command to display the internal DHCP server configuration.

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

Syntax Description	show dhcp	Displays internal DHCP server configuration information.
	leases	Enter leases to display allocated DHCP leases.
	summary	Enter summary to display DHCP summary information.
	scope	Enter the name of a scope to display the DHCP information for that scope.

Defaults None.

Examples

```
> show dhcp leases
```

```
No leases allocated.
```

```
> show dhcp summary
```

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

```
> show dhcp 003
```

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

Related Commands **config dhcp**

show dhcp proxy

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

show dhcp proxy

Syntax Description	show dhcp proxy Displays the status of DHCP proxy handling.
Defaults	None.
Examples	<pre>> show dhcp proxy DHCP Proxy Behaviour: enabled</pre>
Related Commands	config dhcp proxy

show eventlog

Use the **show eventlog** command to display the event log.

show eventlog

Syntax Description	show	Displays configurations.
	eventlog	System events.

Defaults	None.

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

Related Commands	show msglog

show exclusionlist

To display a summary of all clients on the manual exclusion list (blacklisted) from associating with this Cisco Wireless LAN controller, use the **show exclusionlist** command. A list containing each manually Excluded MAC address is displayed.

show exclusionlist

Syntax Description

show	Displays configurations.
exclusionlist	Manual exclusion list.

Defaults

None.

Examples

```
> show exclusionlist
```

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

Related Commands

config exclusionlist add
config exclusionlist delete
config exclusionlist description
show client

show guest-lan

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

show guest-lan *guest_lan_id*



Note Enter **show guest-lan summary** to view all wired guest LANs configured on the controller.

Syntax Description

show	Displays configurations.
guest-lan	Indicates the active wired guest LAN.

Defaults

None.

Examples

> **show guest-lan 2**

```

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

```

Related Commands

show guest-lan summary
show client summary guest-lan

show hreap group detail

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

```
show hreap group detail group_name
```

Syntax Description	show hreap	Displays configurations.
	group detail	Displays details of the hybrid-REAP group details.

Defaults	None.

```
Examples
> show hreap group detail 192.12.1.2

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

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

Related Commands	show hreap group summary

show hreap group summary

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

show hreap group summary

Syntax Description	show hreap	Displays configurations
	group summary	Displays a summary of the hybrid-REAP group.

Defaults	None.

Examples	> show hreap group summary
	HREAP Group Summary: Count 1
	Group Name # APs
	Group 1 1

Related Commands	show hreap group detail

show ike

Use the **show ike** command to display active IKE SAs.

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

Syntax Description

show	Command action.
ike	Displays active IKE SAs.
brief	List of all active IKE SAs.
<i>IP_or_MAC_address</i>	IP or MAC address of active IKE SA.

Defaults

None.

Examples

```
> show ike
```

Related Commands

None.

show interface

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

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

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

Defaults None.

Examples

> **show interface summary**

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



Note The interface name of the wired guest LAN in this example is *wired-guest* and its VLAN ID is 236.

> **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 **config interface**

show inventory

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

show inventory

Syntax Description	show	Displays configurations.
	inventory	Physical Cisco Wireless LAN controller configuration.

Defaults	None.

Examples

> **show inventory**

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

**Note**

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.

Related Commands	show sysinfo

show ipsec

Use the **show ipsec** command to display active IPsec SAs.

```
show ipsec {brief | IP_or_MAC_address}
```

Syntax Description	show	Command action.
	ipsec	Displays active IPsec SAs
	{brief	Enter brief to display active IPsec SAs.
	IP_or_MAC_address}	Enter the IP address of MAC address of an IPsec SA.

Defaults	None.

Examples	> show ipsec brief

Related Commands	None.

show known ap

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

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

Syntax Description	show	Displays configurations.
	known ap	Known Cisco lightweight access point information.
	summary	Displays a list of all known access points.
	detailed	Provides detailed information for all known access points.
	MAC	MAC address of the known AP

Defaults	None.

```
> show known ap summary

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

Related Commands	config ap

show l2tp

To display L2TP sessions, use the **show l2tp** command.

show l2tp {**summary** | *ip_address*}

Syntax Description	show l2tp	Displays configurations.
	summary	Displays all L2TP sessions.
	<i>ip_address</i>	Displays an L2TP session.

Defaults None.

Examples

```
> show l2tp summary

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

```

Related Commands None.

show lag summary

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

show lag summary

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> show lag summary
```

LAG Enabled

Related Commands **config lag**

show ldap

To display the detailed LDAP server information, use the **show ldap** command.

show ldap *index*

Syntax Description	<i>index</i>	LDAP server index. Valid values are from 1 to 17.

Defaults	None.

Examples	<pre>> 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</pre>

Related Commands	config ldap show ldap statistics show ldap summary

show ldap statistics

To display the detailed LDAP server information, use the **show ldap statistics** command.

show ldap statistics

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Examples	<pre>> 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 ...</pre>

Related Commands	config ldap show ldap show ldap summary

show ldap summary

To display the current LDAP status, use the **show ldap summary** command.

show ldap summary

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Examples	<pre>> show ldap summary</pre> <table><thead><tr><th>Idx</th><th>Server Address</th><th>Port</th><th>Enabled</th></tr><tr><th>---</th><th>-----</th><th>----</th><th>-----</th></tr></thead><tbody><tr><td>1</td><td>2.3.1.4</td><td>389</td><td>Yes</td></tr><tr><td>2</td><td>10.10.20.22</td><td>389</td><td>Yes</td></tr></tbody></table>	Idx	Server Address	Port	Enabled	---	-----	----	-----	1	2.3.1.4	389	Yes	2	10.10.20.22	389	Yes
Idx	Server Address	Port	Enabled														
---	-----	----	-----														
1	2.3.1.4	389	Yes														
2	10.10.20.22	389	Yes														

Related Commands	config ldap show ldap show ldap statistics

show load-balancing

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

show load-balancing

Syntax Description	show	Displays configurations.
	load-balancing	Displays the load-balancing status.

Defaults	None.

Examples	<pre>> show load-balancing Aggressive Load Balancing..... Enabled Aggressive Load Balancing Window..... 0 clients</pre>

Related Commands	config load-balancing

show local-auth certificates

This command is used to display local authentication certificate information:

show local-auth certificates

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

> **show local-auth certificates**

Certificates available for Local EAP authentication:

Certificate issuer vendor

CA certificate:

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

Certificate issuer cisco

CA certificate:

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

Certificate issuer legacy

CA certificate:

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

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

Related Commands **config local-auth eap-profile**

show local-auth config

This command is used to display local authentication configuration information:

show local-auth config

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> show local-auth config
User credentials database search order:
  Primary ..... Local DB

Configured EAP profiles:
  Name ..... fast-test
  Certificate issuer ..... default
  Enabled methods ..... fast
  Configured on WLANs ..... 2

EAP Method configuration:
EAP-TLS:
  Certificate issuer ..... default
  Peer verification options:
    Check against CA certificates ..... Enabled
    Verify certificate CN identity .... Disabled
    Check certificate date validity ... Enabled
EAP-FAST:
  TTL for the PAC ..... 3 600
  Initial client message ..... <none>
  Local certificate required ..... No
  Client certificate required ..... No
  Vendor certificate required ..... No
  Anonymous provision allowed ..... Yes
  Authenticator ID ..... 7b7fffff000000000000000000000000
  Authority Information ..... Test

EAP Profile..... tls-prof
  Enabled methods for this profile ..... tls
  Active on WLANs ..... 1 3
EAP Method configuration:
EAP-TLS:
  Certificate issuer used ..... cisco
  Peer verification options:
    Check against CA certificates ..... disabled
    Verify certificate CN identity .... disabled
    Check certificate date validity ... disabled
```

Related Commands

config local-auth eap-profile
config local-auth method fast

show local-auth statistics

This command is used to display local EAP authentication statistics:

show local-auth statistics

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> show local-auth statistics
```

Local EAP authentication DB statistics:

```
Requests received ..... 14
Responses returned ..... 14
Requests dropped (no EAP AVP) ..... 0
Requests dropped (other reasons) ..... 0
Authentication timeouts ..... 0
```

Authentication statistics:

Method	Success	Fail
Unknown	0	0
LEAP	0	0
EAP-FAST	2	0
EAP-TLS	0	0
PEAP	0	0

Local EAP credential request statistics:

```
Requests sent to LDAP DB ..... 0
Requests sent to File DB ..... 2
Requests failed (unable to send) ..... 0
Authentication results received:
  Success ..... 2
  Fail ..... 0
```

Certificate operations:

```
Local device certificate load failures ..... 0
Total peer certificates checked ..... 0
Failures:
  CA issuer check ..... 0
  CN name not equal to identity ..... 0
  Dates not valid or expired ..... 0
```

Related Commands

- clear stats local-auth**
- config local-auth eap-profile**
- config local-auth method fast**

show location

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

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

Syntax Description

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

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> show location summary
Location Summary

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

Related Commands

clear location rfid
config location

show location statistics rfid

To see any RFID-related errors, use the **show location statistics rfid** command.

show location statistics rfid

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Examples > **show location statistics rfid**

RFID Statistics

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

Related Commands **clear location statistics rfid**

show logging

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

show logging

Syntax Description	show	Displays configurations.
	logging	Current parameters and buffer content details.

Defaults None.

Examples

> **show logging**

```

Logging to buffer :
- Logging of system messages to buffer :
  - Logging filter level..... errors
  - Number of system messages logged..... 67227
  - Number of system messages dropped..... 21136
- Logging of debug messages to buffer ..... Disabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
Logging to console :
- Logging of system messages to console :
  - Logging filter level..... errors
  - Number of system messages logged..... 0
  - Number of system messages dropped..... 88363
- Logging of debug messages to console ..... Enabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
Logging to syslog :
- Syslog facility..... local0
- Logging of system messages to syslog :
  - Logging filter level..... errors
  - Number of system messages logged..... 67227
--More-- or (q)uit
  - Number of system messages dropped..... 21136
- Logging of debug messages to syslog ..... Disabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
- Number of remote syslog hosts..... 0
  - Host 0..... Not Configured
  - Host 1..... Not Configured
  - Host 2..... Not Configured
Logging of traceback..... Disabled
Logging of process information..... Disabled
Logging of source file informational..... Enabled
Timestamping of messages.....
  - Timestamping of system messages..... Enabled
  - Timestamp format..... Date and Time
  - Timestamping of debug messages..... Enabled
  - Timestamp format..... Date and Time

Logging buffer (67227 logged, 21136 dropped)

*Apr 03 09:48:01.728: %MM-3-INVALID_PKT_RECVD: mm_listen.c:5508 Received an invalid

```

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

Related Commands

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

show login session

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

show login session

Syntax Description

show	Displays configurations.
login session	Current session details.

Defaults

None.

Examples

```
> show login session
```

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

Related Commands

config login session close

show lwapp reap association

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

show lwapp reap association

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Examples	> show lwapp reap association

Related Commands	show lwapp reap status

show lwapp reap status

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

show lwapp reap status

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Examples	> show lwapp reap status

Related Commands	show lwap reap association

show macfilter

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

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

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

Defaults None.

Examples

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

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

```
> show macfilter summary
```

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

Local Mac Filter Table

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

Related Commands

- config macfilter mac-delimiter**
- config macfilter add**
- config macfilter delete**
- config macfilter description**
- config macfilter wlan-id**

show mgmtuser

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

show mgmtuser

Syntax Description

show	Displays configurations.
mgmtuser	List of management users.

Defaults

None.

Examples

```
> show mgmtuser
```

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

Related Commands

config mgmtuser add, config mgmtuser delete, config mgmtuser password

Show Mobility Commands

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

show mobility anchor

To display the wireless LAN anchor list for the Cisco Wireless LAN controller mobility groups, use the **show mobility anchor** command.

show mobility anchor

Syntax Description

show	Displays configurations.
mobility	Mobility group.
anchor	Displays the mobility wireless LAN anchor list.

Defaults

None.

Examples

```
> show mobility anchor

Mobility Anchor Export List
WLAN ID      IP Address
```

Related Commands

config mobility group discovery
config mobility group member

show mobility anchor {wlan | guest-lan}

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 {wlan | guest-lan}** command.

show mobility anchor {wlan | guest-lan} {wlan_id | guest_lan_id}

Syntax Description

show	Displays configurations.
mobility	Mobility group.
anchor	Displays the mobility wireless LAN anchor list.
wlan	Wireless LAN parameters.
guest-lan	Indicates the active wired guest LAN.
<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 16.
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Defaults

None.

Examples

```
> show mobility anchor {wlan | guest-lan} 5
```

```
Mobility Anchor Export List
WLAN ID      IP Address Status
  1          10.50.234.2  UP
  1          10.50.234.6  UP
  2          10.50.234.2  UP
  2          10.50.234.3  CNTRL_DATA_PATH_DOWN

GLAN ID      IP Address Status
  1          10.20.100.2  UP
  2          10.20.100.3  UP
```

The status field 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.

Related Commands

```
show mobility summary
config mobility group keepalive count
config mobility group keepalive interval
config mobility group anchor add {wlan | guest-lan}
```

```
config {wlan | guest-lan} mobility anchor add  
config {wlan | guest-lan} mobility anchor delete  
config mobility group anchor delete {wlan | guest-lan}
```

show mobility statistics

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

show mobility statistics

Syntax Description

show	Displays configurations.
mobility	Mobility group.
statistics	Displays statistics for the mobility manager.

Defaults

None.

Examples

> **show mobility statistics**

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

Related Commands

config mobility group discovery, config mobility group member

show mobility summary

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

show mobility summary

Syntax Description

show	Displays configurations.
mobility	Mobility group.
summary	Displays a summary of the mobility manager.

Defaults

None.

Examples

> **show mobility summary**

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

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



Note

Some WLAN controllers may list no mobility security mode.

Related Commands

config mobility group discovery
config mobility group member

show msglog

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

show msglog

Syntax Description	show	Displays configurations.
	msglog	Shows message logs.

Defaults None.

Examples

```
> show msglog
```

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

Related Commands **show eventlog**

show nac statistics

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

show nac statistics

Syntax Description	show	Displays configurations.
	nac	Network access control.
	statistics	Detailed statistics.

Defaults None.

Examples

```
> show nac statistics

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

Related Commands

show nac acl

show nac summary

show nac summary

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

show nac summary

Syntax Description

show	Displays configurations.
nac	Network Access Control.
summary	Summary information.

Defaults

None.

Examples

```
> show nac summary
```

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

Related Commands

show nac acl

show nac statistics

show netuser

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

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

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

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

Command Default	This command has no defaults.

Command History	Release	Modification
	4.1	This command was revised to include detail and summary options.

Examples

```
> show netuser summary
```

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

```
> show netuser detail john10
```

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

Related Commands	config netuser maxeapuserlogin
	show netuser summary

show netuser guest-roles

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

show netuser guest-roles

Syntax Description

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

Command Default

This command has no defaults.

Examples

> **show netuser guest-roles**

```

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

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

```

Related Commands

config netuser maxcapuserlogin
show netuser summary

show network summary

To display the network configuration of the Cisco Wireless LAN controller, use the **show network summary** command.

show network summary

Syntax Description	show	Displays configurations.
	network	Network configuration.
	summary	Summary of network configuration.

Defaults	None.

Examples

```
> show network summary
```

```
RF-Network Name..... mrf
Web Mode..... Enable
Secure Web Mode..... Enable
Secure Web Mode Cipher-Option High..... Disable
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable
Ethernet Broadcast Mode..... Disable
IGMP snooping..... Disabled
IGMP timeout..... 60 seconds
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
Cisco AP Default Master..... Disable
AP Join Priority..... Enabled
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..... Disable
Apple Talk ..... Disable
AP Fallback ..... Enable
Web Auth Redirect Ports ..... 80
Fast SSID Change ..... Disabled
802.3 Bridging ..... Disable
```

Related Commands	config ap priority config network ap-priority config network arptimeout config network bcast-ssid config network broadcast config network dsport config network master-base

config network mgmt-via-wireless
config network multicast global
config network params
config network rf-mobility-domain
config network secureweb
config network secweb-passwd
config network ssh
config network telnet
config network usertimeout
config network vlan
config network webmode

show network multicast mgid detail

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

show network multicast mgid detail *mgid_value*

Syntax Description	show	Displays configurations.
	network	Network configuration.
	<i>mgid_value</i>	Number between 550 and 4095.

Defaults None.

Examples

```
> show network multicast mgid detail

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

Related Commands **show network multicast mgid summary**

show network multicast mgid summary

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

show network multicast mgid summary

Syntax Description

show	Displays configurations.
network	Network configuration.

Defaults

None.

Examples

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

```
Layer2 MGID Mapping:
```

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

```
Layer3 MGID Mapping:
```

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

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

Related Commands

show network multicast mgid detail

show nmsp notify-interval summary

To display the NMSP configuration settings, use the **show nmsp notify-interval summary** command.

Syntax Description	This command has no arguments or keywords.

Defaults	None

Examples	<pre>>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</pre>

Related Commands	config nmsp notify-interval measurement

show nmosp statistics

To display NMSP coutners., use the **show nmosp statistics** command.

show nmosp statistics {summary | connection all}

Syntax Description

show	Displays configurations.
nmosp statistics	Displays NMSP coutners.
summary	Displays common NMSP counters.
connection all	Displays all connection-specific counters.

Defaults

This command has no defaults.

Examples

```
> show nmosp statistics summary
```

Related Commands

clear locp statistics

show nmsp status

To display the status of active NMSP connections, use the **show nmsp status** command.

show nmsp status

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Examples	<pre>>show nmsp status</pre> <table border="0"><thead><tr><th>LocServer IP</th><th>TxEchoResp</th><th>RxEchoReq</th><th>TxData</th><th>RxData</th></tr><tr><th>-----</th><th>-----</th><th>-----</th><th>-----</th><th>-----</th></tr></thead><tbody><tr><td>10.19.35.51</td><td>34100</td><td>34100</td><td>6</td><td>6</td></tr></tbody></table>	LocServer IP	TxEchoResp	RxEchoReq	TxData	RxData	-----	-----	-----	-----	-----	10.19.35.51	34100	34100	6	6
LocServer IP	TxEchoResp	RxEchoReq	TxData	RxData												
-----	-----	-----	-----	-----												
10.19.35.51	34100	34100	6	6												

Related Commands	clear locp statistics

show pmk-cache

To display information about the PMK cache, use the **show port** command.

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

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

Defaults None.

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

> show pmk-cache all

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

Related Commands config pmk-cache delete

show port

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

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

Syntax Description

show	Displays configurations.
port	Cisco Wireless LAN controller port.
{ <i>port</i> summary }	Individual port or all ports.

Defaults

None.

Examples

> **show port 1**

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



Note

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

> **show port summary**

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



Note

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

Related Commands

config ap port
config network dsport
config mirror port
config port adminmode
config port linktrap
config port power

show qos queue_length all

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

show qos queue_length all

Syntax Description

show	Displays configurations.
qos	Quality of Service information.
queue_length all	Displays queue lengths.

Defaults

None.

Examples

```
> show qos queue_length all
```

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

Related Commands

config qos

Show Radius Commands

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

show radius acct statistics

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

show radius acct statistics

Syntax Description	show	Displays configurations.
	radius acct	RADIUS accounting server.
	statistics	Displays RADIUS accounting server statistics.

Defaults None.

Examples

> **show radius acct statistics**

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

Related Commands

- show radius auth statistics**
- show radius summary**

show radius auth statistics

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

show radius auth statistics

Syntax Description

show	Displays configurations.
radius auth	RADIUS authentication server.
statistics	Displays RADIUS authentication server statistics.

Defaults

None.

Examples

> **show radius auth statistics**

```

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

```

Related Commands

show radius acct statistics
show radius summary

show radius rfc3576 statistics

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

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

show radius rfc3576 statistics

Syntax	Description
show	Displays configurations.
radius rfc3576	RADIUS RFC3576 server.
statistics	Displays RADIUS RFC-3576 server statistics.

Defaults None.

Examples

```
> show radius rfc3576 statistics
```

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

Related Commands

- show radius auth statistics**
- show radius summary**
- show radius rfc3576**

show radius summary

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

show radius summary

Syntax Description

show	Displays configurations.
radius	RADIUS authentication server.
summary	Server summary.

Defaults

None.

Examples

```
> show radius summary
```

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

Authentication Servers

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

Accounting Servers

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

Related Commands

show radius auth statistics

show radius acct statistics

Show RFID Commands

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

show rfid client

To list the RFID tags that are associated to the controller as clients, use the **show rfid client** command.

show rfid client

Syntax Description This command has no arguments or keywords.

Command Default This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

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

> **show rfid client**

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



Note

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

Related Commands

- config rfid
- show rfid config
- show rfid detail
- show rfid summary

show rfid config

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

show rfid config

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> show rfid config

RFID Tag Data Collection ..... Enabled
RFID Tag Auto-Timeout ..... Enabled
RFID Client Data Collection ..... Disabled
RFID Data Timeout ..... 200 seconds
```

Related Commands

- config rfid
- show rfid detail
- show rfid summary

show rfid detail

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

show rfid detail *mac_address*

Syntax Description

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

Command Default

This command has no defaults.

Examples

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

RFID address..... 00:12:b8:00:20:52
Vendor..... G2
Last Heard..... 51 seconds ago
Packets Received..... 2
Bytes Received..... 324
Cisco Type.....

Content Header
=====
Version..... 0
Tx Power..... 12 dBm
Channel..... 1
Reg Class..... 12
Burst Length..... 1

CCX Payload
=====
Last Sequence Control..... 0
Payload length..... 127
Payload Data Hex Dump

01 09 00 00 00 00 0b 85 52 52 52 02 07 4b ff ff
7f ff ff ff 03 14 00 12 7b 10 48 53 c1 f7 51 4b
50 ba 5b 97 27 80 00 67 00 01 03 05 01 42 34 00
00 03 05 02 42 5c 00 00 03 05 03 42 82 00 00 03
05 04 42 96 00 00 03 05 05 00 00 00 55 03 05 06
42 be 00 00 03 02 07 05 03 12 08 10 00 01 02 03
04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 03 0d 09 03
08 05 07 a8 02 00 10 00 23 b2 4e 03 02 0a 03

Nearby AP Statistics:
  lap1242-2(slot 0, chan 1) 50 seconds ag.... -76 dBm
  lap1242(slot 0, chan 1) 50 seconds ago..... -65 dBm
```

Related Commands

config rfid
show rfid config

show rfid summary

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

show rfid summary

Syntax Description This command has no arguments or keywords.

Command Default This command has no defaults.

Release	Modification
4.1	This command was introduced.

Examples

```
> show rfid summary
```

```
Total Number of RFID : 5
```

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

Related Commands

- config rfid
- show rfid config
- show rfid detail

Show Rogue Adhoc Commands

Use the **rogue adhoc** commands rogue adhoc settings.

show rogue adhoc detailed

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

show rogue adhoc detailed *MAC*

Syntax Description	show	Displays configurations.
	rogue adhoc	Ad-hoc rogue.
	detailed	Displays detailed information.
	MAC	Ad-hoc rogue MAC address.

Defaults None.

Examples

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

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

Related Commands **show rogue adhoc summary**

show rogue adhoc summary

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

show rogue adhoc summary

Syntax Description

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

Defaults

None.

Examples

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

Client MAC Address    Adhoc BSSID    State  #  APs    Last Heard
-----
xx:xx:xx:xx:xx:xx    super          Alert  1          Sat Aug  9 21:12:50 2004
xx:xx:xx:xx:xx:xx          Alert  1          Aug  9 21:12:50 2003
xx:xx:xx:xx:xx:xx          Alert  1          Sat Aug  9 21:10:50 2003
```

Related Commands

show rogue adhoc detailed

Show Rogue AP Commands

Use the **rogue ap** commands to display rogue access point settings.

show rogue ap clients

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

show rogue ap clients *ap_mac_address*

Syntax Description	show	Displays configurations.
	rogue ap	Rogue access point.
	clients	Summary information.
	<i>ap_mac_address</i>	Rogue access point MAC address.

Defaults None.

Examples

```
> show rogue ap clients xx:xx:xx:xx:xx:xx
MAC Address State # Aps Last Heard
-----
00:bb:cd:12:ab:ff Alert 1 Fri Nov 30 11:26:23 2007
```

Related Commands **show rogue ap summary**

show rogue ap detailed

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

show rogue ap detailed *ap_mac_address*

Syntax Description

show	Displays configurations.
rogue ap	Rogue access point.
detailed	Displays detailed information.
<i>ap_mac_address</i>	Rogue access point MAC address.

Defaults

None.

Examples

```
> show rogue ap detailed xx:xx:xx:xx:xx:xx
```

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

Related Commands

show rogue ap summary
show rogue ap clients

show rogue ap summary

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

show rogue ap summary

Syntax	Description
show	Displays configurations.
rogue ap	Rogue access point.
summary	Displays a list of all rogue access points.

Defaults None.

Examples

> **show rogue ap summary**

```
Rogue Location Discovery Protocol..... Disabled
Rogue ap timeout..... 1200

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

Related Commands

- show rogue ap detailed**
- show rogue ap clients**
- show rogue ap friendly summary**
- show rogue ap malicious summary**
- show rogue ap unclassified summary**

show rogue ap friendly summary

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

show rogue ap friendly summary

Syntax Description

show	Displays configurations.
rogue ap	Rogue access point.
friendly	Friendly rogue access points
summary	Displays a list of all rogue access points.

Defaults

None.

Examples

```
> show rogue ap friendly summary
```

```
Number of APs..... 1
MAC Address      State      # APs # Clients Last Heard
-----
00:0a:b8:7f:08:c0 Internal      1      0 Tue Nov 27 13:52:04 2007
```

Related Commands

show rogue ap detailed
show rogue ap clients
show rogue ap malicious summary
show rogue ap summary
show rogue ap unclassified summary

show rogue ap malicious summary

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

show rogue ap malicious summary

Syntax Description

show	Displays configurations.
rogue ap	Rogue access point.
malicious	Malicious rogue access points
summary	Displays a list of all rogue access points.

Defaults

None.

Examples

```
> show rogue ap malicious summary
```

```
Number of APs..... 2
MAC Address          State          # APs # Clients Last Heard
-----
XX:XX:XX:XX:XX:XX Alert              1      0 Tue Nov 27 13:52:04 2007
XX:XX:XX:XX:XX:XX Alert              1      0 Tue Nov 27 13:52:04 2007
```

Related Commands

show rogue ap detailed
show rogue ap clients
show rogue ap friendly summary
show rogue ap summary
show rogue ap unclassified summary

show rogue ap unclassified summary

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

show rogue ap unclassified summary

Syntax Description

show	Displays configurations.
rogue ap	Rogue access point.
unclassified	Unclassified rogue access points
summary	Displays a list of all rogue access points.

Defaults

None.

Examples

```
> show rogue ap unclassified summary
```

```
Number of APs..... 164
MAC Address      State                # APs # Clients Last Heard
-----
00:0b:85:63:cd:bd Alert                1      0    Fri Nov 30 11:12:52 2007
00:0b:85:63:cd:e7 Alert                1      0    Fri Nov 30 11:29:01 2007
00:0b:85:63:ce:05 Alert                1      0    Fri Nov 30 11:26:23 2007
00:0b:85:63:ce:07 Alert                1      0    Fri Nov 30 11:26:23 2007
```

Related Commands

show rogue ap detailed
show rogue ap clients
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap summary
show rogue ap unclassified summary

Show Rogue Client Commands

Use the following **rogue client** commands to display the rogue client settings.

show rogue client detailed

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

show rogue client detailed *MAC*

Syntax Description

show	Displays configurations.
rogue client	Rogue client.
detailed	Provide detailed information for a rogue client.
MAC	Rogue client MAC address.

Defaults

None.

Examples

```
> show rogue client detailed xx:xx:xx:xx:xx:xx

Rogue BSSID..... 00:0b:85:23:ea:d1
State..... Alert
First Time Rogue was Reported..... Mon Dec 3 21:50:36 2007
Last Time Rogue was Reported..... Mon Dec 3 21:50:36 2007
Rogue Client IP address..... Not known
Reported By
AP 1
MAC Address..... 00:15:c7:82:b6:b0
Name..... AP0016.47b2.31ea
Radio Type..... 802.11a
RSSI..... -71 dBm
SNR..... 23 dB
Channel..... 149
Last reported by this AP..... Mon Dec 3 21:50:36 2007
```

Related Commands

show rogue client summary

show rogue client summary

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

show rogue client summary

Syntax Description

show	Displays configurations.
rogue client	Rogue client.
summary	Displays a list of all rogue clients.

Defaults

None.

Examples

> **show rogue client summary**

MAC Address	State	#	APs	Last	Heard
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:00:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:09:11	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:03:11	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:03:11	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:09:11	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	18:57:08	2005
xx:xx:xx:xx:xx:xx	Alert	1	Thu Aug 4	19:12:08	2005

Related Commands

show rogue client detailed

show rogue ignore-list

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

show rogue ignore-list

Syntax Description	show	Displays configurations.
	rogue ignore-list	Rogue access points that are configured to be ignored.
	summary	Displays a list of all rogue clients.

Defaults None.

Examples

```
> show rogue client summary

MAC Address
-----
XX:XX:XX:XX:XX:XX
```

Related Commands **show rogue client detailed**

Show Rogue Rule Commands

Use the following **rogue rule** commands to display the rogue rule settings.

show rogue rule detailed

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

show rogue rule detailed *rule_name*

Syntax Description	show	Displays configurations.
	rogue rule	Rogue rules.
	detailed	Shows detailed information on a specific rogue classification rule.
	<i>rule_name</i>	Rogue rule name.

Defaults None.

Examples

```
> show rogue rule detailed Rule2

Priority..... 2
Rule Name..... Rule2
State..... Enabled
Type..... Malicious
Match Operation..... Any
Hit Count..... 352
Total Conditions..... 2
Condition 1
type..... Client-count
value..... 10
Condition 2
type..... Duration
value (seconds)..... 2000
```

Related Commands **show rogue rule detailed**

show rogue rule summary

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

show rogue rule summary

Syntax Description	show	Displays configurations.
	rogue rule	Rogue rules.
	summary	Displays a list of all rogue rules that are configured on the controller

Defaults None.

Examples

```
> show rogue rule summary
```

Priority	Rule Name	State	Type	Match	Hit Count
1	mtest	Enabled	Malicious	All	0
2	asdfasdf	Enabled	Malicious	All	0

Related Commands **show rogue rule detailed**

show route summary

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

show route summary

Syntax Description	show route	Command action.
	summary	Displays all the configured routes.

Defaults	None.

Examples

> **show route summary**

Number of Routes..... 1

Destination Network	Genmask	Gateway
-----	-----	-----
xxx.xxx.xxx.xxx	255.255.255.0	xxx.xxx.xxx.xxx

Related Commands	config route

show rules

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

show rules

Syntax Description	show rules Displays active internal firewall rules.
Defaults	None.
Examples	<pre> > 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) ----- ... </pre>
Related Commands	None.

show run-config

To show a comprehensive view of the current Cisco Wireless LAN controller configuration, use the **show run-config** command.

show run-config

Syntax Description	show run-config	Command action.

Defaults	None.

Examples

> show run-config

Press Enter to continue...

System Inventory

Switch Description..... Cisco Controller

Machine Model.....

Serial Number..... FLS0923003B

Burned-in MAC Address..... xx:xx:xx:xx:xx:xx

Crypto Accelerator 1..... Absent

Crypto Accelerator 2..... Absent

Power Supply 1..... Absent

Power Supply 2..... Present, OK

Press Enter to continue Or <Ctl Z> to abort...



Note

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.

Related Commands	config route

show serial

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

show serial

Syntax	Description
show	Displays configurations.
serial	Displays EIA-232 parameters and serial port inactivity timeout.

Defaults 9600, 8, off, 1, none.

Examples

```
> 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 show the console port login timeout and maximum number of simultaneous Command Line Interface (CLI) sessions, use the **show sessions** command.

show sessions

Syntax Description	show	Displays configurations.
	sessions	Displays CLI session configuration information.

Defaults 5 minutes, 5 sessions.

Examples

```
> show sessions

CLI Login Timeout (minutes)..... 0
Maximum Number of CLI Sessions..... 5
```

The response indicates that the CLI sessions never time out and that the Cisco Wireless LAN controller can host up to five simultaneous CLI sessions.

Related Commands

config sessions maxsessions

config sessions timeout

show services mobility

To view all mobility services active on the controller, use the **show services mobility** command.

show services mobility {**summary** | **detail** {**all** | *ipaddr*}}

Syntax Description		
show		Displays configurations.
services mobility		Displays mobility services.
summary		Displays summary of mobility services.
detail		Displays mobility services in detail.
all		Displays details for all connections.
<i>ipaddr</i>		Displays details for the specified IP connection.

Defaults None.

Examples

```
show services mobility summary
Mobility Services Subscribed:

Server          IP Services
10.19.35.218    Client Tracking, Tag Tracking
```

show snmpcommunity

To display SNMP community entries, use the **show snmpcommunity** command.

show snmpcommunity

Syntax Description

show	Displays configurations.
snmpcommunity	Displays SNMP community entries.

Defaults

None.

Examples

```
> show snmpcommunity
```

SNMP Community Name	Client IP Address	Client IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read Only	Enable
*****	0.0.0.0	0.0.0.0	Read/Write	Enable

Related Commands

config snmp version
config snmp community mode
config snmp community accessmode
config snmp community create
config snmp community delete
config snmp community ipaddr

show snmptrap

To show the Cisco Wireless LAN controller SNMP trap receivers and their status, use the **show snmptrap** command.

show snmptrap

Syntax Description	show	Displays configurations.
	snmptrap	SNMP trap receivers.

Defaults	None.

Examples

```
> show snmptrap
```

SNMP Trap Receiver Name	IP Address	Status
-----	-----	-----
xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	Enable

Related Commands

config snmp version
config snmp trapreceiver

show snmpv3user

To show the SNMP version 3 configuration, use the **show snmpv3user** command.

show snmpv3user

Syntax Description

show	Displays configurations.
snmpv3user	SNMP version 3 configuration information.

Defaults

None.

Examples

```
> show snmpv3user
```

SNMP v3 User Name	AccessMode	Authentication	Encryption
-----	-----	-----	-----
default	Read/Write	HMAC-SHA	CFB-AES

Related Commands

config snmp version
config snmp v3user

show snmpversion

To display which versions of Simple Network Management Protocol (SNMP) are enabled or disabled on your controller, use the **show snmpversion** command.

show snmpversion

Syntax Description	show	Display settings.
	snmpversion	Displays SNMP v1/v2/v3c status (enabled or disabled).

Defaults Enable.

Examples

```
> show snmpversion

SNMP v1  Mode..... Disable
SNMP v2c Mode..... Enable
SNMP v3  Mode..... Enable
```

Related Commands [config snmp version](#)

show spanningtree port

To show the Cisco Wireless LAN controller spanning tree port configuration, use the **show spanningtree port** command.

When the a Cisco 4400 Series wireless LAN controller is configured for port redundancy, spanning tree protocol must be disabled for all ports on the Cisco 4400 series wireless LAN controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 series wireless LAN controller.

show spanningtree port *port*

Syntax Description	show	Displays configurations.
	spanningtree	Spanning tree.
	port	Displays spanning tree values on a per port basis.
	<i>port</i>	Physical port number: • 1 through 4 on Cisco 2100 series wireless LAN controller. • 1 or 2 on Cisco 4402 series wireless LAN controller. • 1 through 4 on Cisco 4404 series wireless LAN controller.

**Note**

Some WLAN controllers do not support the spanning tree function.

Defaults

800C, Disabled, 802.1D, 128, 100, Auto.

Examples

> **show spanningtree port 3**

STP Port ID..... 800C
STP Port State..... Disabled
STP Port Administrative Mode..... 802.1D
STP Port Priority..... 128
STP Port Path Cost..... 100
STP Port Path Cost Mode..... Auto

Related Commands

config spanningtree port

show spanningtree switch

To show the Cisco Wireless LAN controller network (DS port) spanning tree configuration, use the **show spanningtree switch** command.

show spanningtree switch

Syntax Description

show	Displays configurations.
spanningtree	Spanning tree.
switch	Displays spanning tree values on a per switch basis.



Note

Some WLAN controllers do not support the spanning tree function.

Defaults

None.

Examples

```
> show spanningtree switch
```

```
STP Specification..... IEEE 802.1D
STP Base MAC Address..... 00:0B:85:02:0D:20
Spanning Tree Algorithm..... Disable
STP Bridge Priority..... 32768
STP Bridge Max. Age (seconds)..... 20
STP Bridge Hello Time (seconds)..... 2
STP Bridge Forward Delay (seconds)..... 15
```

Related Commands

```
config spanningtree switch bridgepriority
config spanningtree switch forwarddelay
config spanningtree switch hellotime
config spanningtree switch maxage
config spanningtree switch mode
```

Show Statistics Commands

Use the **show stats** commands to display controller statistics.

show stats port

To show physical port receive and transmit statistics, use the **show stats port** command.

show stats port {*detailed port* | *summary port*}

Syntax Description	show	Displays configurations.
	stats	Statistics.
	port	Port.
	detailed	Displays detailed port statistics.
	summary	Displays port summary statistics.
	<i>port</i>	Physical port number: • 1 through 4 on Cisco 2100 Series wireless LAN controllers. • 1 or 2 on Cisco 4402 Series wireless LAN controllers. • 1 through 4 on Cisco 4404 Series wireless LAN controllers. • 1 on Cisco WLCM Series wireless LAN controllers.

Defaults None.

Examples

> **show stats port summary 1**

```
Packets Received Without Error..... 399958
Packets Received With Error..... 0
Broadcast Packets Received..... 8350
Packets Transmitted Without Error..... 106060
Transmit Packets Errors..... 0
Collisions Frames..... 0
Time Since Counters Last Cleared..... 2 day 11 hr 16 min 23 sec
```

> **show stats port detailed 1**

```
PACKETS RECEIVED (OCTETS)
Total Bytes..... 267799881
64 byte pkts      :918281
65-127 byte pkts  :354016      128-255 byte pkts  :1283092
256-511 byte pkts :8406        512-1023 byte pkts :3006
1024-1518 byte pkts :1184      1519-1530 byte pkts :0
> 1530 byte pkts  :2

PACKETS RECEIVED SUCCESSFULLY
Total..... 2567987
Unicast Pkts :2547844      Multicast Pkts:0      Broadcast Pkts:20143

PACKETS RECEIVED WITH MAC ERRORS
Total..... 0
Jabbers :0      Undersize :0      Alignment :0
FCS Errors:0      Overruns :0

RECEIVED PACKETS NOT FORWARDED
Total..... 0
```



```

Local Traffic Frames:0                RX Pause Frames      :0
Unacceptable Frames :0                VLAN Membership      :0
VLAN Viable Discards:0                MulticastTree Viable:0
ReserveAddr Discards:0
CFI Discards      :0                Upstream Threshold  :0

PACKETS TRANSMITTED (OCTETS)
Total Bytes..... 353831
64 byte pkts      :0                65-127 byte pkts    :0
128-255 byte pkts :0                256-511 byte pkts   :0
512-1023 byte pkts :0                1024-1518 byte pkts :2
1519-1530 byte pkts :0                Max Info             :1522

PACKETS TRANSMITTED SUCCESSFULLY
Total..... 5875
Unicast Pkts :5868                Multicast Pkts:0        Broadcast Pkts:7

TRANSMIT ERRORS
Total Errors..... 0
FCS Error      :0                TX Oversized :0        Underrun Error:0

TRANSMIT DISCARDS
Total Discards..... 0
Single Coll Frames :0                Multiple Coll Frames:0
Excessive Coll Frame:0                Port Membership      :0
VLAN Viable Discards:0

PROTOCOL STATISTICS
BPDUs Received      :6                BPDUs Transmitted    :0
802.3x RX PauseFrame:0

Time Since Counters Last Cleared..... 2 day 0 hr 39 min 59 sec

```

Related Commands**config port adminmode**

show stats switch

To show the network (DS port) receive and transmit statistics, use the **show stats switch** command.

show stats switch {detailed | summary}

Syntax Description	show	Displays configurations.
	stats	Statistics.
	switch	Cisco Wireless LAN controller.
	detailed	Displays detailed switch statistics.
	summary	Displays switch summary statistics.

Defaults None.

Examples

> **show stats switch summary**

```
Packets Received Without Error..... 136410
Broadcast Packets Received..... 18805
Packets Received With Error..... 0
Packets Transmitted Without Error..... 78002
Broadcast Packets Transmitted..... 3340
Transmit Packet Errors..... 2
Address Entries Currently In Use..... 26
VLAN Entries Currently In Use..... 1
Time Since Counters Last Cleared..... 2 day 11 hr 22 min 17 sec
```

> **show stats switch detailed**

```
RECEIVE
Octets..... 19351718
Total Pkts..... 183468
Unicast Pkts..... 180230
Multicast Pkts..... 3219
Broadcast Pkts..... 19
Pkts Discarded..... 0

TRANSMIT
Octets..... 354251
Total Pkts..... 5882
Unicast Pkts..... 5875
Multicast Pkts..... 0
Broadcast Pkts..... 7
Pkts Discarded..... 0

ADDRESS ENTRIES
Most Ever Used..... 1
Currently In Use..... 1

VLAN ENTRIES
Maximum..... 128
Most Ever Used..... 1
Static In Use..... 1
Dynamic In Use..... 0
```

```
VLANs Deleted..... 0
Time Since Ctrs Last Cleared..... 2 day 0 hr 43 min 22 sec
```

Related Commands**config network dsport**

show switchconfig

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

show switchconfig

Syntax Description	show	Displays configurations.
	switchconfig	Displays parameters that apply to the Cisco Wireless LAN controller.

Defaults

None.

Examples

```
> show switchconfig

802.3x Flow Control Mode..... Disable
Current LWAPP Transport Mode..... Layer 3
LWAPP Transport Mode after next switch reboot.... Layer 3
```

Related Commands

config switchconfig flowcontrol

config switchconfig mode

show sysinfo

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

show sysinfo

Syntax Description	show	Displays configurations.
	sysinfo	Cisco Wireless LAN controller information.

Defaults	None.

Examples	<pre>> show sysinfo Manufacturer's Name..... <company name> Product Name..... Product Version..... 1.2.48.0 RTOS Version..... 1.2.48.0 Bootloader Version..... 1.1.11.0 System Name..... IT2003 System Location..... Andrew 1 System Contact..... Wireless_administrator System ObjectID..... 1.3.6.1.4.1.14179 IP Address..... 172.168.2.36 System Up Time..... 2 days 11 hrs 30 mins 1 secs Configured Country..... United States Operating Environment..... Commercial (0 to 40 C) Internal Temp Alarm Limits..... 0 to 65 C Internal Temperature..... +38 C State of 802.11b Network..... Enabled State of 802.11a Network..... Enabled Number of WLANs..... 2 3rd Party Access Point Support..... Disabled Number of Active Clients..... 1 xxxxxxxxxxxxxxxxxxxx</pre>

Related Commands	config ap, config country config sysname config wlan

show tacacs acct statistics

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

show tacacs acct statistics

Syntax Description	This command has no arguments or keywords.

Command Default	This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> show tacacs acct statistics
```

Accounting Servers:

```

Server Index..... 1
Server Address..... 10.0.0.0
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 1
Retry Requests..... 0
Accounting Response..... 0
Accounting Request Success..... 0
Accounting Request Failure..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... -1
Timeout Requests..... 1
Unknowntype Msgs..... 0
Other Drops..... 0

```

Related Commands	config tacacs
	show tacacs summary

show tacacs athr statistics

This command is used to display TACACS+ server authorization statistics.

show tacacs athr statistics

Syntax Description	This command has no arguments or keywords.

Command Default	This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

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

Related Commands	config tacacs
	show tacacs summary

show tacacs auth statistics

This command is used to display TACACS+ server authentication statistics.

show tacacs auth statistics

Syntax Description	This command has no arguments or keywords.

Command Default	This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> show tacacs auth statistics
```

Authentication Servers:

```

Server Index..... 2
Server Address..... 10.0.0.2
Msg Round Trip Time..... 0 (msec)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0

```

Related Commands	config tacacs show tacacs summary

show tacacs summary

This command is used to display TACACS+ server summary information.

show tacacs summary

Syntax Description This command has no arguments or keywords.

Command Default This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> show tacacs summary
```

Authentication Servers

Idx	Server Address	Port	State	Tout
2	10.0.0.2	6	Enabled	30

Accounting Servers

Idx	Server Address	Port	State	Tout
1	10.0.0.0	10	Enabled	2

Authorization Servers

Idx	Server Address	Port	State	Tout
3	10.0.0.3	4	Enabled	2
...				

Related Commands

- config tacacs
- show tacacs summary

show tech-support

To show Cisco Wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support** command.

show tech-support

Syntax Description	show	Displays configurations.
	tech-support	Displays system resource information.

Defaults	None.

Examples

> **show tech-support**

Current CPU Load..... 0%

System Buffers

Max Free Buffers..... 4608

Free Buffers..... 4604

Buffers In Use..... 4

Web Server Resources

Descriptors Allocated..... 152

Descriptors Used..... 3

Segments Allocated..... 152

Segments Used..... 3

System Resources

Uptime..... 747040 Secs

Total Ram..... 127552 Kbytes

Free Ram..... 19540 Kbytes

Shared Ram..... 0 Kbytes

Buffer Ram..... 460 Kbytes

Related Commands	None.

show time

To show the Cisco Wireless LAN controller time and date, use the **show time** command.

show time

Syntax Description	show	Displays configurations.
	time	Cisco Wireless LAN controller time and date.

Defaults None.

Examples

```
> show time

Time..... Thu Aug  4 19:51:49 2005

Timezone delta..... 0:0
Daylight savings..... disabled

NTP Servers
  NTP Polling Interval..... 86400

      Index          NTP Server
      -----

```

Related Commands **config time**

show trapflags

To show the Cisco Wireless LAN controller SNMP trap flags, use the **show trapflags** command.

show trapflags

Syntax Description	show	Displays configurations.
	trapflags	Displays the Cisco Wireless LAN controller SNMP trap flags.

Defaults	None.

Examples

> **show trapflags**

```

Authentication Flag..... Enable
Link Up/Down Flag..... Enable
Multiple Users Flag..... Enable
Spanning Tree Flag..... Enable

Client Related Traps
    802.11 Disassociation..... Disable
    802.11 Deauthenticate..... Disable
    802.11 Authenticate Failure..... Disable
    802.11 Association Failure..... Disable
    Excluded..... Disable

802.11 Security related traps
    WEP Decrypt Error..... Enable

Cisco AP
    Register..... Enable
    InterfaceUp..... Enable

Auto-RF Profiles
    Load..... Enable
    Noise..... Enable
    Interference..... Enable
    Coverage..... Enable

Auto-RF Thresholds
    tx-power..... Enable
    channel..... Enable
    antenna..... Enable

AAA
    auth..... Enable
    servers..... Enable

rogueap..... Enable

wps..... Enable

configsave..... Enable

IP Security
    esp-auth..... Enable

```

```

esp-replay..... Enable
invalidSPI..... Enable
ike-neg..... Enable
suite-neg..... Enable
invalid-cookie..... Enable

```

Related Commands

config trapflags authentication

config trapflags linkmode

config trapflags multiusers

config trapflags stpmode

config trapflags client

config trapflags ap

config trapflags rrm-profile

config trapflags rrm-params

config trapflags aaa

config trapflags rogueap

config trapflags configsave

config trapflags ipsec

show traplog

show traplog

To show the Cisco Wireless LAN controller SNMP trap log, use the **show traplog** command.

show traplog

Syntax Description

show	Displays configurations.
traplog	Cisco Wireless LAN controller SNMP trap log.

Defaults

None.

Examples

```
> show traplog
```

```
Number of Traps Since Last Reset..... 2447
```

```
Number of Traps Since Log Last Displayed... 2447
```

```
Log System Time          Trap
-----
0 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:52:62:fe detected on Base Rad
io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
b/g) with RSSI: -78 and SNR: 10
1 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:52:19:d8 detected on Base Rad
io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
b/g) with RSSI: -72 and SNR: 16
2 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:26:a1:8d detected on Base Rad
io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
b/g) with RSSI: -82 and SNR: 6
3 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:14:b3:4f detected on Base Rad
io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
b/g) with RSSI: -56 and SNR: 30
```

```
Would you like to display more entries? (y/n)
```

Related Commands

show trapflags

show version

This command is used to display access point's software information .

show version

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

You can only use this command from the access point console port when not connected to a controller.

Examples

```
AP# show version
Cisco IOS Software, C1240 Software (C1240-K9W8-M), Experimental Version
12.3(20060829:081904) [BLD-wnbu_a10_temp_060823.daily 163]
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 30-Aug-06 03:03 by
ROM: Bootstrap program is C1240 boot loader
BOOTLDR: C1240 Boot Loader (C1240-BOOT-M) Version 12.3(7)JA1, RELEASE SOFTWARE (fc1)
Ap1242-2 uptime is 4 minutes
System returned to ROM by power-on
System image file is "flash:/c1240-k9w8-mx.wnbu_a10_temp_060823.20060830d/c1240-k9w8-"
cisco AIR-LAP1242AG-A-K9 processor (revision B0) with 24566K/8192K bytes of memory.
Processor board ID FTX0944B00B
PowerPCElvis CPU at 266Mhz, revision number 0x0950
Last reset from power-on
LWAPP image version 4.1.69.0
1 FastEthernet interface
2 802.11 Radio(s)
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:14:1C:ED:47:14
Part Number : 73-9925-03
PCA Assembly Number : 800-26579-03
PCA Revision Number : A0
PCB Serial Number : FOC09351E0U
Top Assembly Part Number : 800-26804-01
Top Assembly Serial Number : FTX0944B00B
Top Revision Number : A0
Product/Model Number : AIR-LAP1242AG-A-K9
Configuration register is 0xF
```

Related Commands

None.

show watchlist

To display the client watchlist, use the **show watchlist** command.

show watchlist

Syntax Description	show	Command action.
	watchlist	Displays client watchlist entry.

Defaults	None.

Examples	<pre>> show watchlist client watchlist state is disabled</pre>

Related Commands	config watchlist delete
	config watchlist enable
	config watchlist disable
	config watchlist add

show wlan

To display configuration information for a specified wireless LAN or a foreign access point, or to display wireless LAN summary information, use the **show wlan** command.

show wlan [**apgroups** | **summary** | *wlan_id* | **foreignAp**]

Syntax Description		
show		Displays configurations.
wlan		Wireless LAN.
apgroups		Displays access point group information.
summary		Displays a summary of all wireless LANs.
<i>wlan_id</i>		Wireless LAN identifier from 1 to 16.
foreignAp		Displays the configuration for support of foreign access points.

Defaults None.

Examples

```
> show wlan 1
WLAN Identifier..... 1
Profile Name..... wlan
Network Name (SSID)..... wlan
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Admission Control

    NAC-State..... Enabled
    Quarantine VLAN..... 110
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
Webauth DHCP exclusion..... Disabled
Interface..... management
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Allowed
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Peer-to-Peer Blocking Action..... Disabled
Radio Policy..... All
DTIM period for 802.11a radio..... 1
DTIM period for 802.11b radio..... 1
Local EAP Authentication..... Disabled
Security

    802.11 Authentication:..... Open System
    Static WEP Keys..... Disabled
```

```

802.1X..... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Enabled
  WPA (SSN IE)..... Disabled
  WPA2 (RSN IE)..... Enabled
    TKIP Cipher..... Disabled
    AES Cipher..... Enabled
  Auth Key Managent
    802.1x..... Enabled
    PSK..... Disabled
    CCKM..... Disabled
    FT(802.11r)..... Disabled
FT-PSK(802.11r)..... Disabled
FT Reassociation Timeout..... 20
FT Over-The-Air mode..... Enabled
FT Over-The-Ds mode..... Enabled
  CKIP ..... Disabled
  IP Security..... Disabled
  IP Security Passthru..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Conditional Web Redirect..... Disabled
  Splash-Page Web Redirect..... Disabled
  Auto Anchor..... Disabled
  Cranite Passthru..... Disabled
  Fortress Passthru..... Disabled
  H-REAP Local Switching..... Disabled
  Infrastructure MFP protection..... Enabled (Global Infrastructu
MFP Disabled)
  Client MFP..... Optional
  Tkip MIC Countermeasure Hold-down Timer..... 60

Mobility Anchor List
WLAN ID      IP Address      Status
-----
> show wlan summary

Number of WLANs..... 2

WLAN ID  WLAN Profile Name / SSID      Status      Interface Name
-----
1        test / test                      Disabled    management

> show wlan foreignap

Foreign AP support is not enabled.

```

Related Commands **config wlan create**

Show WPS Commands

Use the **show wps** commands to display Wireless Protection System (WPS) settings.

show wps

To display the Wireless Protection System configuration on the controller, use the **show wps** command.

show wps {ap-authentication summary | signature summary | summary}

Syntax Description	show	Command action.
	wps	Display WPS configuration.
	ap-authentication summary	Display AP neighbor WPS authentication.
	signature summary	Display the WPS signature summary.
	summary	Display the WPS summary.

Defaults None.

Examples

```
> show wps ap-authentication summary
```

```
AP neighbor authentication is <disabled>.
```

```
Authentication alarm threshold is 1.
```

```
RF-Network Name: <B1>
```

```
> 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:
                0:0x00c0:0x03ff
                4:0x01:0x01
```

```
Signature-ID..... 1
Precedence..... 2
Signature Name..... NULL probe resp 1
Type..... Standard
FrameType..... management
State..... enabled
Action..... report
Tracking..... per Signature and Mac
Signature Frequency..... 50 pkts/interval
Signature Mac Frequency..... 30
pkts/intervalInterval..... 1 sec
```

```

Quiet Time..... 300 sec
Description..... NULL Probe Response - Zero length SSID
element
Patterns:
                0:0x0050:0x03ff
                36:0x0000:0xffff

```

> **show wps summary**

```

Client Exclusion Policy
  Excessive 802.11-association failures..... Enabled
  Excessive 802.11-authentication failures..... Enabled
  Excessive 802.1x-authentication..... Enabled
  Network access control failure..... Enabled
  IP-theft..... Enabled
  Excessive Web authentication failure..... Enabled

Trusted AP Policy
  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
    Automatically contain rogues advertising .... Alarm Only
    Detect Ad-Hoc Networks..... Alarm Only
  Rogue Clients
    Validate rogue clients against AAA..... Disabled
    Detect trusted clients on rogue APs..... Alarm Only
  Rogue AP timeout..... 1200

Signature Policy
  Signature Processing..... Enabled

```

Related Commands

```

show wps ap-authentication
show wps cids-sensor detail
show wps cids-sensor summary
show wps mfp
show wps shun-list
show wps signature events {standard | custom}
show wps signature events summary
show wps signature summary
show wps summary
config wps ap-authentication
config wps cids-sensor
config wps mfp
config wps rogue-ap
config wps shun-list
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  
debug wps
```

show wps ap-authentication

To display the access point neighbor authentication configuration on the controller, use the **show wps ap-authentication** command.

show wps ap-authentication summary

Syntax Description

show	Command action.
wps	Displays WPS configuration.
ap-authentication	AP neighbor authentication config
summary	Displays the WPS summary.

Defaults

None.

Examples

```
> show wps ap-authentication summary
```

```
AP neighbor authentication is <disabled>.
```

```
Authentication alarm threshold is 1.
```

```
RF-Network Name: <B1>
```

Related Commands

[show wps](#)
[show wps cids-sensor detail](#)
[show wps cids-sensor summary](#)
[show wps summary](#)
[config wps ap-authentication](#)
[config wps cids-sensor](#)
[config wps rogue-ap](#)

show wps cids-sensor detail

To display detailed information on a specified WPS IDS sensor, use the **show wps cids-sensor detail** command.

show wps cids-sensor detail *index*

Syntax Description	<i>index</i>	Specifies the IDS sensor index value.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> show wps cids-sensor detail 1
```

```
IP Address..... 10.0.0.51
Port..... 443
Query Interval..... 60
Username..... Sensor_user1
Cert Fingerprint..... SHA1: 00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00
Query State..... Disabled
Last Query Result..... Unknown
Number of Queries Sent..... 0
```

Related Commands

[show wps](#)
[show wps ap-authentication](#)
[show wps cids-sensor summary](#)
[show wps summary](#)
[config wps ap-authentication](#)
[config wps cids-sensor](#)

show wps cids-sensor summary

To display IDS sensor summary information, use the **show wps cids-sensor summary** command.

show wps cids-sensor summary

Syntax Description This command has no arguments or keywords.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> show wps summary
```

Configured IDS Sensors

Index	Server Address	Port	State	Intvl	Last Query
-----	-----	-----	-----	-----	-----
1	10.0.0.51	443	Disabled	60	Unknown

Related Commands

[show wps](#)
[show wps ap-authentication](#)
[show wps cids-sensor detail](#)
[show wps summary](#)
[config wps ap-authentication](#)
[config wps cids-sensor](#)

show wps mfp

To display Management Frame Protection (MFP) information, use the **show wps mfp** command.

show wps mfp {summary | statistics}

Syntax Description	show	Command action.
	wps	Displays WPS configuration.
	mfp	Displays Management Frame Protection information.
	summary	Displays MFP configuration and status.
	statistics	Displays MFP statistics.

Examples

> **show wps mfp summary**

```
Global Infrastructure MFP state..... DISABLED (*all infrastructure
settings are overridden)
Controller Time Source Valid..... False
```

WLAN ID	WLAN Name	WLAN Status	Infra. Protection	Client Protection
1	homeap	Disabled	*Enabled	Optional but inactive (WPA2 not configured)
2	7921	Enabled	*Enabled	Optional but inactive (WPA2 not configured)
3	open1	Enabled	*Enabled	Optional but inactive (WPA2 not configured)
4	7920	Enabled	*Enabled	Optional but inactive (WPA2 not configured)

AP Name	Infra. Validation	Radio	Operational State	--Infra. Capability-- Protection	Validation
AP1252AG-EW	*Enabled	b/g a	Down Down	Full Full	Full Full

>**show wps mfp statistics**

BSSID	Radio Validator AP	Last Source Addr	Found	Error Type	Count	Frame Types
no errors						

Related Commands

[show wps ap-authentication](#)
[show wps cids-sensor detail](#)
[show wps cids-sensor summary](#)
[show wps summary](#)
[config wps ap-authentication](#)
[config wps cids-sensor](#)
[config wps rogue-ap](#)
[config wps mfp](#)

show wps shun-list

To display 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	> show wps shun-list

Related Commands	config wps shun-list

show wps signature events {standard | custom}

To display more information on the attacks detected by a particular standard or custom signature, use the **show wps signature events summary** command.

show wps signature events {standard | custom} precedence# summary

show wps signature events {standard | custom} precedence# detailed per-signature source_mac

show wps signature events {standard | custom} precedence# detailed per-mac source_mac

Syntax Description

standard custom	Specifies the type of IDS signature to display.
precedence#	Specifies the signature precedence identification.
summary	Displays tracking signature summary information.
detailed	Displays tracking source MAC address detail information.
per-signature	Displays MAC address tracking information per signature source.
source_mac	Specifies the MAC address of the source.
per-mac	Displays MAC address tracking information per MAC address source.

Examples

To display information on the attacks detected by standard signature 1, use this command:

```
> show wps signature events standard 1 summary
```

```
Precedence..... 1
Signature Name..... Bcast deauth
Type..... Standard
Number of active events..... 2

Source MAC Addr    Track Method    Frequency #    APs    Last Heard
-----
00:a0:f8:58:60:dd  Per Signature   50            1      Wed Oct 25 15:03:05 2006
00:a0:f8:58:60:dd  Per Mac        30            1      Wed Oct 25 15:02:53 2006
```

Related Commands

[config wps signature](#)
[config wps signature frequency](#)
[config wps signature interval](#)
[config wps signature mac-frequency](#)
[config wps signature quiet-time](#)
[config wps signature reset](#)
[show wps signature events summary](#)
[show wps signature summary](#)
[show wps summary](#)

show wps signature events summary

To see the number of attacks detected by the enabled signatures, use the **show wps signature events summary** command.

show wps signature events summary

Syntax Description

This command has no arguments or keywords.

Examples

```
> show wps signature events summary
```

Precedence	Signature Name	Type	# Events
1	Bcast deauth	Standard	2
2	NULL probe resp 1	Standard	1

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 {standard | custom}](#)
- [show wps signature summary](#)
- [show wps summary](#)

show wps signature summary

To see individual summaries of all of the standard and custom signatures installed on the controller, use the **show wps signature summary** command.

show wps signature summary

Syntax Description	This command has no arguments or keywords.

Examples

```
> show wps signature summary

Signature-ID..... 1
Precedence..... 1
Signature Name..... Bcast deauth
Type..... standard
FrameType..... management
State..... enabled
Action..... report
Tracking..... per Signature and Mac
Signature Frequency..... 50 pkts/interval
Signature Mac Frequency..... 30 pkts/interval
Interval..... 1 sec
Quiet Time..... 300 sec
Description..... Broadcast Deauthentication Frame
Patterns:
    0 (Header) : 0x00c0:0x00ff
    4 (Header) : 0x01:0x01
...
```

Related Commands

[config wps signature](#)
[config wps signature frequency](#)
[config wps signature interval](#)
[config wps signature mac-frequency](#)
[config wps signature quiet-time](#)
[config wps signature reset](#)
[show wps signature events {standard | custom}](#)
[show wps signature events summary](#)
[show wps summary](#)

show wps summary

To display WPS summary information, use the **show wps summary** command.

show wps summary

Syntax Description

This command has no arguments or keywords.

Examples

> **show wps summary**

```
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 {standard | custom}](#)
[show wps signature events summary](#)
[show wps signature summary](#)

Configuring Controller Settings

Use the config commands to configure Cisco Wireless LAN controller options and settings.

Config 802.11x Commands

Use the **config 802.11x** commands to configure settings for an 802.11a, 802.11b, or other supported 802.11 network.

config {802.11a | 802.11b} 11nsupport

To enable 802.11n support on the network, use the **config {802.11a | 802.11b} 11nsupport** command.

config {802.11a | 802.11b} 11nsupport {enable | disable}

Syntax	Description
config	Configure parameters.
802.11a	802.11a Cisco radio.
802.11b	802.11b Cisco radio.
11nsupport	Support for 802.11n devices.
enable	Enable support.
disable	Disable support.

Defaults None.

Examples

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

Related Commands

- config {802.11a | 802.11b} 11nsupport mcs tx
- config {802.11a | 802.11b} 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 {802.11a | 802.11b} 11nsupport a-mpdu tx priority

To specify the aggregation method used for 802.11n packets, use the **config {802.11a | 802.11b} 11nsupport a-mpdu tx priority** command.

config {802.11a | 802.11b} 11nsupport a-mpdu tx priority {0-7 | all} {enable | disable}



Note Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). A-MPDU is performed in the software whereas A-MSDU is performed in the hardware.

Syntax Description

config	Configure parameters.
802.11a	802.11a Cisco radio.
802.11b	802.11b Cisco radio.
11nsupport	Support for 802.11n devices.
a-mpdu tx priority	Aggregated MAC Protocol Data Unit priority levels assigned per traffic type: • 1—Background • 2—Spare • 0—Best effort • 3—Excellent effort • 4—Controlled load • 5—Video, less than 100-ms latency and jitter • 6—Voice, less than 10-ms latency and jitter • 7—Network control • all—Configure all of the priority levels at once. Note Configure the priority levels to match the aggregation method used by the clients.
enable	The traffic associated with the priority level uses A-MPDU transmission.
disable	The traffic associated with the priority level uses A-MSDU transmission.

Defaults

All priorities, except 5 and 6, are enabled by default. Priorities 5 and 6 are disabled by default.

Examples

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

Related Commands

config {802.11a | 802.11b} 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 {802.11a | 802.11b} 11nsupport antenna

To use of specific antennas for a particular access point, enter this command:

```
config {802.11a | 802.11b} 11nsupport antenna {tx | rx} Cisco_AP {A | B | C} {enable | disable}
```

Syntax Description		
config		Configure parameters.
802.11a		802.11a Cisco radio.
802.11b		802.11b Cisco radio.
11nsupport antenna		Support for 802.11n devices.
tx		Enable the antenna to transmit.
rx		Enable the antenna to receive.
<i>Cisco_AP</i>		Specify the access point.
A B C		The antenna ports. A is the right antenna port, B is the left antenna port, and C is the center antenna port.
enable		Enable support.
disable		Disable support.

Defaults None.

Examples `config 802.11a 11nsupport antenna tx AP1 C enable`

Related Commands

- config {802.11a | 802.11b} 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 {802.11a | 802.11b} 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 {802.11a | 802.11b} 11nsupport mcs tx** command.

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

Syntax	Description
config	Configure parameters.
802.11a	802.11a Cisco radio.
802.11b	802.11b Cisco radio.
11nsupport	Support for 802.11n devices.
mcs tx	Modulation and coding scheme data rates: • 0 (7 Mbps) • 1 (14 Mbps) • 2 (21 Mbps) • 3 (29 Mbps) • 4 (43 Mbps) • 5 (58 Mbps) • 6 (65 Mbps) • 7 (72 Mbps) • 8 (14 Mbps) • 9 (29 Mbps) • 10 (43 Mbps) • 11 (58 Mbps) • 12 (87 Mbps) • 13 (116 Mbps) • 14 (130 Mbps) • 15 (144 Mbps)
enable	Enable support.
disable	Disable support.

Defaults None.

Examples
 > config 802.11a 11nsupport mcs tx 5 enable

Related Commands
 config {802.11a | 802.11b} 11nsupport
 config wlan wmm required

config {802.11a | 802.11b} 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 {802.11a | 802.11b} cac video acm

To enable or disable video Call Admission Control (CAC) for the 802.11a or 802.11b/g network, use the **config {802.11a | 802.11b} cac video acm** command.

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

Syntax Description

config	Configure parameters.
802.11a 802.11b	802.11a or 802.11b Cisco radio.
cac	Call Admission Control parameters.
video	Video traffic parameters.
acm	Admission control.
enable disable	Enable or disable video CAC.

Defaults

Disabled.

Usage Guidelines

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

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

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

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

Examples

```
> config 802.11a cac video acm enable
> config 802.11b cac video acm disable
```

Related Commands

config {802.11a | 802.11b} cac video max-bandwidth
config {802.11a | 802.11b} cac video roam-bandwidth
config {802.11a | 802.11b} cac video tspec-inactivity-timeout

config {802.11a | 802.11b} 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 {802.11a | 802.11b} cac video max-bandwidth** command.

config {802.11a | 802.11b} cac video max-bandwidth *bandwidth*

Syntax Description

config	Configure parameters.
802.11a 802.11b	802.11a or 802.11b Cisco radio.
cac	Call Admission Control parameters.
video	Video traffic parameters.
max-bandwidth	Specify the percentage of the maximum allocated bandwidth for video applications on the selected radio band.
<i>bandwidth</i>	A bandwidth percentage value from 0-100%.

Defaults

0%

Usage Guidelines

The maximum radio frequency (RF) bandwidth cannot exceed 100% for voice + video. Once the client reaches the value specified, the access point rejects new calls on this network.



Note

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

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

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

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

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

Examples

```
> config 802.11a cac video max-bandwidth 50
> config 802.11b cac video max-bandwidth 75
```

Related Commands

config {802.11a | 802.11b} cac video acm

config {802.11a | 802.11b} cac video roam-bandwidth

config {802.11a | 802.11b} cac video tspec-inactivity-timeout

config {802.11a | 802.11b} 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 {802.11a | 802.11b} cac video roam-bandwidth** command.

config {802.11a | 802.11b} cac video roam-bandwidth *bandwidth*

Syntax Description

config	Configure parameters.
802.11a 802.11b	802.11a or 802.11b Cisco radio.
cac	Call Admission Control parameters.
video	Video traffic parameters.
roam-bandwidth	Specify the percentage of the maximum allocated bandwidth reserved for roaming video clients on the selected radio band.
<i>bandwidth</i>	A bandwidth percentage value from 0 to 25%.

Defaults

0%

Usage Guidelines

The controller reserves the specified bandwidth from the maximum allocated bandwidth for roaming video clients.



Note If this parameter is set to zero (0), the controller assumes that the operator does not want to do any bandwidth allocation and, therefore, allows all bandwidth requests.

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

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

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

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

Examples

```
> config 802.11a cac video roam-bandwidth 10
> config 802.11b cac video roam-bandwidth 0
```

Related Commands**config {802.11a | 802.11b} cac video acm****config {802.11a | 802.11b} cac video max-bandwidth****config {802.11a | 802.11b} cac video tspec-inactivity-timeout**

config {802.11a | 802.11b} cac video tspec-inactivity-timeout

To process or ignore the WMM traffic specifications (TSPEC) inactivity timeout received from an access point, use the **config {802.11a | 802.11b} cac video tspec-inactivity-timeout** command.

config {802.11a | 802.11b} cac video tspec-inactivity-timeout {enable | ignore}

Syntax Description

config	Configure parameters.
802.11a 802.11b	802.11a or 802.11b Cisco radio.
cac	Call Admission Control parameters.
video	Video traffic parameters.
tspec-inactivity-timeout	Specify the response to TSPEC inactivity timeout messages received from an access point.
enable ignore	Process or ignore the TSPEC inactivity timeout messages.

Defaults

Disabled (ignore).

Usage Guidelines

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

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

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

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

Examples

```
> config 802.11a cac video tspec-inactivity-timeout enable
> config 802.11b cac video tspec-inactivity-timeout ignore
```

Related Commands

```
config {802.11a | 802.11b} cac video acm
config {802.11a | 802.11b} cac video max-bandwidth
config {802.11a | 802.11b} cac video roam-bandwidth
```

config {802.11a | 802.11b} 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 {802.11a | 802.11b} cac voice acm** command.

config {802.11a | 802.11b} cac voice acm {enable | disable}

Syntax Description

config	Configure parameters.
802.11a 802.11b	802.11a or 802.11b Cisco radio.
cac	Call Admission Control parameters.
voice	Voice traffic parameters.
acm	Admission control.
enable disable	Enable or disable bandwidth-based CAC.

Defaults

Disabled.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

```
> config 802.11a cac voice acm enable
> config 802.11b cac voice acm disable
```

Related Commands

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

config {802.11a | 802.11b} 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 {802.11a | 802.11b} cac voice max-bandwidth** command.

config {802.11a | 802.11b} cac voice max-bandwidth *bandwidth*

Syntax Description		
config		Configure parameters.
802.11a 802.11b		802.11a or 802.11b Cisco radio.
cac		Call Admission Control parameters.
voice		Voice traffic parameters.
max-bandwidth		Specify the percentage of the maximum allocated bandwidth for voice applications on the selected radio band.
<i>bandwidth</i>		A bandwidth percentage value from 40-85%.

Defaults 75%

Command History	Release	Modification
	4.1	This command was introduced.

Usage Guidelines The maximum radio frequency (RF) bandwidth cannot exceed 100% for voice + video. Once the client reaches the value specified, the access point rejects new calls on this network.

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

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

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

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

Examples

```
> config 802.11a cac voice max-bandwidth 50
> config 802.11b cac voice max-bandwidth 75
```

Related Commands

config {802.11a | 802.11b} {enable | disable} network
config {802.11a | 802.11b} cac voice acm
config {802.11a | 802.11b} cac voice load-based
config {802.11a | 802.11b} cac voice roam-bandwidth
config {802.11a | 802.11b} cac voice stream-size
config {802.11a | 802.11b} cac voice tspec-inactivity-timeout
config {802.11a | 802.11b} exp-bwreq
config {802.11a | 802.11b} tsm
config wlan {enable | disable}
save config
show wlan
show wlan summary

config {802.11a | 802.11b} 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 {802.11a | 802.11b} cac voice roam-bandwidth** command.

config {802.11a | 802.11b} cac voice roam-bandwidth *bandwidth*

Syntax Description

config	Configure parameters.
802.11a 802.11b	802.11a or 802.11b Cisco radio.
cac	Call Admission Control parameters.
voice	Voice traffic parameters.
roam-bandwidth	Specify the percentage of the maximum allocated bandwidth reserved for roaming voice clients on the selected radio band.
<i>bandwidth</i>	A bandwidth percentage value from 0 to 25%.

Defaults

6%

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

The maximum radio frequency (RF) bandwidth cannot exceed 100% for voice + video. The controller reserves the specified bandwidth from the maximum allocated bandwidth for roaming voice clients.



Note

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

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

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

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

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

Examples

```
> config 802.11a cac voice roam-bandwidth 10
> config 802.11b cac voice roam-bandwidth 6
```

Related Commands

```
config {802.11a | 802.11b} cac voice acm
config {802.11a | 802.11b} cac voice load-based
config {802.11a | 802.11b} cac voice max-bandwidth
config {802.11a | 802.11b} cac voice stream-size,
config {802.11a | 802.11b} cac voice tspec-inactivity-timeout,
```

config {802.11a | 802.11b} cac voice tspec-inactivity-timeout

To process or ignore the WMM traffic specifications (TSPEC) inactivity timeout received from an access point, use the **config {802.11a | 802.11b} cac voice tspec-inactivity-timeout** command.

config {802.11a | 802.11b} cac voice tspec-inactivity-timeout {enable | ignore}

Syntax Description

config	Configure parameters.
802.11a 802.11b	802.11a or 802.11b Cisco radio.
cac	Call Admission Control parameters.
voice	Voice traffic parameters.
tspec-inactivity-timeout	Specify the response to TSPEC inactivity timeout messages received from an access point.
enable ignore	Process or ignore the TSPEC inactivity timeout messages.

Defaults

Disabled (ignore).

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

```
> config 802.11a cac voice tspec-inactivity-timeout enable
> config 802.11b cac voice tspec-inactivity-timeout ignore
```

Related Commands

config {802.11a | 802.11b} cac voice acm,
config {802.11a | 802.11b} cac voice load-based

config {802.11a | 802.11b} cac voice max-bandwidth
config {802.11a | 802.11b} cac voice roam-bandwidth
config {802.11a | 802.11b} cac voice stream-size

config {802.11a | 802.11b} cac voice load-based

To enable or disable load-based CAC for the 802.11a or 802.11b/g network, use the **config {802.11a | 802.11b} cac voice load-based** command.

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

Syntax Description

config	Configure parameters.
802.11a 802.11b	802.11a or 802.11b Cisco radio.
cac	Call Admission Control parameters.
voice	Voice traffic parameters.
load-based	Load-based CAC parameters.
enable disable	Enable or disable load-based CAC.

Defaults

Disabled.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

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

Related Commands

config {802.11a | 802.11b} cac voice acm
config {802.11a | 802.11b} cac voice max-bandwidth

config {802.11a | 802.11b} cac voice roam-bandwidth

config {802.11a | 802.11b} cac voice stream-size

config {802.11a | 802.11b} cac voice tspec-inactivity-timeout

config {802.11a | 802.11b} cac voice stream-size

To configure the number of aggregated voice WMM traffic specification (TSPEC) streams at a specified data rate for the 802.11a or 802.11b/g network, use the **config {802.11a | 802.11b} cac voice stream-size** command.

config {802.11a | 802.11b} cac voice stream-size *number max-streams mean_datarate*

Syntax Description

config	Configure parameters.
802.11a 802.11b	802.11a or 802.11b Cisco radio.
cac	Call Admission Control parameters.
voice	Voice traffic parameters.
stream-size	Configures the number of voice streams that the controller supports.
number	Specifies the number (1 to 5) of voice streams.
max-streams	Configures the mean data rate of a voice stream.
mean_datarate	Specifies the mean data rate (84 to 91.2 Kbps) of a voice stream.

Defaults

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

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

```
> config 802.11a cac voice stream-size 5 max-streams size 85
> config 802.11b cac voice stream-size 3 max-streams size 90
```

Related Commands

config {802.11a | 802.11b} cac voice acm
config {802.11a | 802.11b} cac voice load-based
config {802.11a | 802.11b} cac voice max-bandwidth
config {802.11a | 802.11b} cac voice roam-bandwidth
config {802.11a | 802.11b} cac voice tspec-inactivity-timeout
config {802.11a | 802.11b} exp-bwreq

config {802.11a | 802.11b} chan_width

To configure the channel width for a particular access point, enter this command:

```
config {802.11a | 802.11b} chan_width Cisco_AP {20 | 40}
```

Syntax Description		
config		Configure parameters.
802.11a		802.11a Cisco radio.
802.11b		802.11b Cisco radio.
chan_width		The channel width for a particular access point
<i>Cisco_AP</i>		Specify the access point.
20		Allows the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels.
40		Allows 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together.

Defaults

Default channel width is **20**.

Usage Guidelines

This parameter can be configured only if the primary channel is statically assigned.

Cisco recommends that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference can occur.

Statically configuring an access point's radio for 20- or 40-MHz mode overrides the globally configured DCA channel width setting (configured using the [config advanced 802.11a channel dca chan-width-11n](#) command). If you ever change the static configuration back to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

Examples

```
> config 802.11a chan_width cisco_ap 40
```

Related Commands

```
config {802.11a | 802.11b} 11nsupport
config wlan wmm required
config {802.11a | 802.11b} 11nsupport 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 {802.11a | 802.11b} disable

To disable the 802.11a or 802.11b/g network before changing pico cell mode parameters, enter this command:

```
config {802.11a | 802.11b} disable
```

Syntax Description

config	Configure parameters.
802.11a	802.11a Cisco radio.
802.11b	802.11b Cisco radio.
disable	Disable support.

Defaults

None.

Examples

```
> config {802.11a | 802.11b} disable
```

Related Commands

```
config 802.11a disable network
config 802.11a channel ap
config 802.11b channel ap
config 802.11a txpower ap
config 802.11a chan_width
```

config {802.11a | 802.11b} l2roam rf-params

To configure 802.11a or 802.11b/g Layer 2 client roaming parameters, enter this command:

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

Syntax Description

config	Configure parameters.
802.11a	802.11a Cisco radio.
802.11b	802.11b/g Cisco radio.
l2roam	Support for Layer 2 client roaming.
rf-params	Radio frequency parameters.
default	Restores Layer 2 client roaming RF parameters to default values.
custom	Configures custom Layer 2 client roaming RF parameters.
<i>min_rssi</i>	The minimum received signal strength indicator (RSSI) that is required for the client to associate to the access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. The valid range is –80 to –90 dBm, and the default value is –85 dBm.
<i>roam_hyst</i>	The hysteresis value indicates how much greater the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between the two access points. The valid range is 2 to 4 dB, and the default value is 2 dB.
<i>scan_thresh</i>	The scan threshold value is the minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold. The valid range is –70 to –77 dBm, and the default value is –72 dBm.
<i>trans_time</i>	The transition time is the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold. The valid range is 1 to 10 seconds, and the default value is 5 seconds. Note For high-speed client roaming applications in outdoor mesh environments, Cisco recommends that you set the transition time to 1 second.

Defaults

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

Usage Guidelines

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

Examples

```
> config 802.11a l2roam rf-params custom -80 2 -70 7
```

Related Commands

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

config {802.11a | 802.11b} picocell

To enable or disable pico cell mode parameters, enter this command:

```
config {802.11a | 802.11b} picocell {enable | disable}
```

Syntax Description

config	Configure parameters.
802.11a	802.11a Cisco radio.
802.11b	802.11b Cisco radio.
picocell	Picocell version 1.
enable	Enable support.
disable	Disable support.

Defaults

None.

Examples

```
> config {802.11a | 802.11b} picocell enable
```

Related Commands

```
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 802.11a chan_width
config {802.11a | 802.11b} disable
config {802.11a | 802.11b} picocell-V2 {enable|disable}
```

config {802.11a | 802.11b} picocell-V2

To enable or disable pico cell version 2 mode parameters, enter this command:

```
config {802.11a | 802.11b} picocell-V2 {enable | disable}
```

Syntax Description		
config		Configure parameters.
802.11a		802.11a Cisco radio.
802.11b		802.11b Cisco radio.
picocell-V2		Picocell version 2.
enable		Enable support.
disable		Disable support.

Defaults None.

Examples

```
> config {802.11a | 802.11b} picocell enable
```

Related Commands

- 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 802.11a chan_width
- config {802.11a | 802.11b} disable
- config {802.11a | 802.11b} picocell {enable|disable}

Config 802.11a Commands

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

config 802.11a antenna extAntGain

To configure the 802.11a external antenna gain, use the **config 802.11a antenna extAntGain** command.

```
config 802.11a antenna extAntGain antenna_gain Cisco_AP
```

Syntax Description	config	Configure parameters.
	802.11a antenna	Antennas for 802.11a Cisco radio.
	extAntGain	Configure external antenna gain.
	<i>antenna_gain</i>	Enter 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 802.11a antenna extAntGain** command, disable the 802.11a Cisco radio with the **config 802.11a disable** command.

After you configure the external antenna gain, use the **config 802.11a enable** command to enable the 802.11a Cisco radio.

Examples To configure the 802.11a external antenna gain for AP1:

```
> config 802.11a antenna extAntGain 1 AP1
```

- Related Commands
- config 802.11a disable
 - config 802.11a enable
 - config 802.11a diversity
 - config 802.11a antenna mode
 - config 802.11a selection

config 802.11a antenna diversity

To configure the diversity option for 802.11a antennas, use the **config 802.11a antenna diversity** command.

config 802.11a antenna diversity {enable | sideA | sideB} Cisco_AP

Syntax Description		
config		Configure parameters.
802.11a antenna diversity		Diversity antennas for 802.11a.
enable		Between the two internal antennas.
sideA		Between the internal antennas and an external antenna connected to the Cisco lightweight access point right port.
sideB		Between the internal antennas and an external antenna connected to the Cisco lightweight access point left port.
<i>Cisco_AP</i>		Cisco lightweight access point name.

Defaults None.

Examples

To enable diversity for AP01:

```
> config 802.11a antenna diversity enable AP01
```

To enable diversity for AP01 using an external antenna connected to the Cisco lightweight access point Left port (sideA).

```
> config 802.11a antenna diversity sideA AP01
```

Related Commands

show ap config 802.11a
 config 802.11a disable
 config 802.11a enable
 config 802.11a extAntGain
 config 802.11a antenna mode
 config 802.11a selection.

config 802.11a antenna mode

To configure the Cisco lightweight access point to use one internal antenna for an 802.11a sectorized 180-degree coverage pattern, or both internal antennas for an 802.11a 360-degree omnidirectional pattern, use the **config 802.11a antenna mode** command.

config 802.11a antenna mode { omni | sectorA | sectorB } *Cisco_AP*

Syntax Description	config	Configure parameters.
	802.11a antenna mode	Antenna for 802.11a Cisco radio.
	omni	Use both internal antennas.
	sectorA	Use only the Side A internal antenna.
	sectorB	Use only the Side B internal antenna.
	<i>Cisco_AP</i>	Cisco lightweight access point name.

Defaults None.

Examples > **config 802.11a antenna mode omni AP01**

Related Commands

show ap config 802.11a

config 802.11a disable

config 802.11a enable

config 802.11a diversity

config 802.11a antenna extAntGain

config 802.11a selection

config 802.11a antenna selection

To configure the 802.11a antenna selection (internal or external), use the **config 802.11a antenna selection** command.

```
config 802.11a antenna selection {internal | external} Cisco_AP
```

Syntax Description		
config		Configure parameters.
802.11a antenna selection		Antenna selection (internal or external) for 802.11a.
internal		Select internal antennas.
external		Select external antenna.
<i>Cisco_AP</i>		Cisco lightweight access point name.

Defaults	None.

Examples	> config 802.11a antenna selection internal AP02

Related Commands	show ap config 802.11a config 802.11a disable config 802.11a enable config 802.11a extAntGain config 802.11a diversity config 802.11a antenna mode.

config 802.11a beaconperiod

In Cisco wireless LAN solution 802.11a networks, all Cisco lightweight access point wireless LANs broadcast a beacon at regular intervals. This beacon notifies clients that 802.11a service is available, and allows the clients to synchronize with the lightweight access point. To change the 802.11a beacon period for the whole 802.11a network, use the **config 802.11a beaconperiod** command.

Before you change the beacon period using the config 802.11a beaconperiod command, make sure that you have disabled the 802.11a network using the config 802.11a disable command. When you are done changing the beacon period, remember to enable the 802.11a network using the config 802.11a enable command.

config 802.11a beaconperiod *time_units*

Syntax	Description
config	Configure parameters.
802.11a	802.11a network parameters.
beaconperiod	Send a beacon every 20 to 1000 milliseconds.
<i>time_units</i>	Beacon interval in time units (TU). One TU is 1024 micro seconds.

Defaults	None.

Examples	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 802.11a channel

To configure an 802.11a network or a single access point for automatic or manual channel selection, use the **config 802.11a channel** command.

config 802.11a channel { **global** [**auto** | **once** | **off**] } [{**AP** *ap_name* [**global** | **channel**] }

When configuring 802.11a channels for a single lightweight access point, use the **config 802.11a disable** command to disable the 802.11a network. Then use the **config 802.11a channel** command to set automatic channel selection by Radio Resource Management (RRM) or manually set the channel for the 802.11a radio. Then enable the 802.11a network using the **config 802.11a enable** command.



Note Refer to the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the channels supported by your access point. The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

Syntax Description

global	Configures the 802.11a operating channel for all lightweight access points.
auto	Specifies the channel is automatically set by radio resource management (RRM) for the 802.11a radio.
once	Specifies the channel is automatically set once by RRM.
off	Specifies the automatic channel selection by RRM is disabled.
ap	Configures the 802.11a operating channel for a specified lightweight access point.
<i>ap_name</i>	Specifies the access point name.
global	Specifies the 802.11a operating channel is automatically set by RRM and over-rides the existing configuration setting.
<i>channel</i>	Specifies a manual channel number to be used by the access point. The supported channels depend on the specific access point used and the regulatory region.

Defaults

This command has no defaults.

Examples

To configure all 802.11a channels for automatic channel configuration by the RRM based on availability and interference, use this command:

```
> config 802.11a channel global auto
```

To have RRM automatically reconfigure all 802.11a channels one time based on availability and interference, use this command:

```
> config 802.11a channel global once
```

To turn 802.11a automatic channel configuration off, use this command:

```
> config 802.11a channel global off
```

To configure all 802.11a channels in access point (AP01) for automatic channel configuration, use this command:

```
> config 802.11a channel AP01 global
```

To configure 802.11a channel 36 in access point AP01 as the default channel, use this command:

```
> config 802.11a channel AP01 36
```

Related Commands

show 802.11a

config 802.11a disable

config 802.11a enable

config 802.11b channel

config country

config 802.11a channel ap

To set the channel for the access point, use the **config 802.11a channel ap** command.

```
config 802.11a channel ap Cisco_AP
```

Syntax Description	config 802.11b channel	Configures the 802.11b radio channels for all access points or a specified access point.
	ap	Configures the 802.11a operating channel for a specified lightweight access point.
	<i>Cisco_AP</i>	Specifies the name of the Cisco access point.

Defaults This command has no defaults.

Examples > config 802.11a channel ap ap01

Related Commands

- show 802.11a
- config 802.11a disable
- config 802.11a enable
- config 802.11b channel
- config country

config 802.11a/802.11b disable

To disable 802.11a transmission for the whole network or for an individual Cisco radio, use the **config 802.11a disable** command. This command can be used any time the CLI interface is active.



Note

You must use this command to disable the network before using many config 802.11a/b commands.

config 802.11a disable network

config 802.11b disable network

config 802.11a disable *Cisco_AP*

Syntax Description

config	Configure parameters.
802.11a	802.11a network parameters.
disable	Disables 802.11a transmission.
network	Disables transmission for the entire 802.11a network.
<i>Cisco_AP</i>	Disables transmission for an individual Cisco lightweight access point radio.

Defaults

Transmission is enabled for the entire network by default.

Examples

To disable the entire 802.11a network:

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

To disable AP01 802.11a transmissions:

```
> config 802.11a 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 802.11a dtpc

To configure the 802.11a DTPC setting, use the **config 802.11a dtpc** command.

config 802.11a dtpc {enable | disable}

Syntax Description	
config	Configure parameters.
802.11a	802.11a network parameters.
dtpc	Dynamic Transmit Power Control.
{enable disable}	- Enter enable to enable DTPC setting configuration. - Enter disable to disable DTPC setting configuration.

Defaults Enabled by default.

Examples > **config 802.11a dtpc disable**

Related Commands

- show 802.11a**
- config 802.11a beaconperiod**
- config 802.11a disable**
- config 802.11a enable**

config 802.11a enable

Enable 802.11a transmissions for the whole network or for an individual Cisco lightweight access point using the **config 802.11a enable** command. You must use this command to enable the network after configuring other 802.11a parameters.

Note that this command only enables the Cisco wireless LAN solution 802.11a network. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual wireless LAN, use the **config wlan radio** command.

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

config 802.11a enable network

config 802.11a enable *Cisco_AP*

Syntax Description

config	Configure parameters.
802.11a	802.11a network parameters.
enable	Disables/enables 802.11a.
network	For the whole network.
<i>Cisco_AP</i>	Override the network setting for an individual Cisco lightweight access point radio.

Defaults

Network = enabled.

Examples

To enable the whole 802.11a network:

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

To enable AP1 802.11a transmissions:

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

To configure the CCX version 5 expedited bandwidth request feature for the 802.11a radio, use the **config 802.11a exp-bwreq** command. When this command is enabled, the controller configures all joining access points for this feature.

config 802.11a exp-bwreq [enable | disable]

Syntax Description

enable	Enables the expedited bandwidth request feature.
disable	Configures the mean datarate of a voice stream.

Defaults

The expedited bandwidth request feature is disabled by default.

Command History

Release	Modification
4.1	This command was introduced.

Examples

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

Cannot change Exp Bw Req mode while 802.11a network is opeational.

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

Related Commands

```
show 802.11a
show ap stats 802.11a
```

config 802.11a fragmentation

To configure the 802.11a fragmentation threshold, use the **config 802.11a fragmentation** command. This command can only be used when the network is not in operation.

config 802.11a fragmentation *threshold*

Syntax Description	config	Configure parameters.
	802.11a	802.11a network parameters.
	fragmentation	Fragmentation threshold.
	<i>threshold</i>	Fragmentation threshold value.

Defaults	None.

Examples	> config 802.11a fragmentation 6500

Related Commands	config 802.11b fragmentation show 802.11b , show ap auto-rtf

config 802.11a pico-cell

To enable or disable the 802.11a pico-cell extensions, use the **config 802.11a pico-cell** command.

This command can only be used when the network is not operational.

config 802.11a pico-cell {enable | disable}

Syntax Description	config	Configure parameters.
	802.11a	802.11a network parameters.
	pico-cell	Pico cell extensions.
	{enable disable}	Enable or disable.

Defaults	None.

Examples	> config 802.11a pico-cell enable

Related Commands	config 802.11b pico-cell config 802.11a, show 802.11a

config 802.11a rate

To set 802.11a mandatory and supported operational rates, use the **config 802.11a rate** command.

The data rates set here are negotiated between the client and the Cisco Wireless LAN controller. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Cisco Wireless LAN controller, any associated client that also supports that rate may communicate with the Cisco lightweight access point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate.

```
config 802.11a rate { disabled | mandatory | supported } rate
```

Syntax Description	config	Configure parameters.
	802.11a	802.11a network parameters.
	rate	Set data rate.
	{ disabled mandatory supported }	• Enter disabled to disable a rate. • Enter mandatory to set a rate to mandatory. • Enter supported to set a rate to supported.
	rate	6, 9, 12, 18, 24, 36, 48, or 54 Mbps.

Defaults None.

Examples To set 802.11a transmission at a mandatory rate at 12 Mbps:

```
> config 802.11a rate mandatory 12
```

Related Commands show ap config 802.11a

 config 802.11b rate

config 802.11a txPower

To configure the 802.11a transmit power level for an automatic or a manual setting for all access points or a single access point, use the **config 802.11a txPower** command.

```
config 802.11a txPower {global [ auto | once | power_level ] } |
{ ap ap_name [ global | power_level ] }
```



Note Refer to the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the maximum transmit power limits for your access point. The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

Syntax Description		
global		Configures the 802.11a transmit power level for all lightweight access points.
auto		Specifies the power level is automatically set by radio resource management (RRM) for the 802.11a Cisco radio.
once		Specifies the power level is automatically set once by RRM.
<i>power_level</i>		Specifies the transmit power level number. The supported power levels depends on the specific access point used and the regulatory region. For example, the 1240 series access point supports 8 levels and the 1200 series access point supports 6 levels.
ap		Configures the 802.11a transmit power level for a specified lightweight access point.
<i>ap_name</i>		Specifies the access point name.
global		Specifies the 802.11a transmit power level is automatically set by RRM and over-rides the existing configuration setting.
<i>power_level</i>		Specifies a manual transmit power level number to be used by the access point. The supported power levels depends on the specific access point used and the regulatory region. For example, the 1240 series access point supports 8 levels and the 1200 series access point supports 6 levels.

Defaults

The command default (global, auto) is for automatic configuration by RRM.

Examples

To have RRM automatically set the 802.11a radio transmit power level in all lightweight access points, use this command:

```
> config 802.11a txPower global auto
```

To manually set the 802.11a radio transmit power to level 5 for all lightweight access points, use this command:

```
> config 802.11a txPower global 5
```

To have RRM automatically set the 802.11a radio transmit power for access point AP1, use this command:

```
> config 802.11a txPower AP1 global
```

To set manually set the 802.11a radio transmit power to power level 2 for access point AP1, use this command:

```
> config 802.11a txPower AP1 2
```

Related Commands

show ap config 802.11a

config 802.11b txPower

config country

config 802.11a txpower ap

To set the transmit power level for the access point, use the **config 802.11a txpower ap** command.

config 802.11a txpower ap *Cisco_AP power_level*

Syntax Description	config 802.11a txPower ap	Configures 802.11a radio transmit power for all lightweight access points or a single access point.
	<i>power_level</i>	Specifies the transmit power level number. The supported power levels depends on the specific access point used and the regulatory region. For example, the 1240 series access point supports 8 levels and the 1200 series access point supports 6 levels.

Defaults None.

Examples To set 802.11a transmission at a mandatory rate at 12 Mbps:
 > **config 802.11a txpower ap ap02 4**

Related Commands

- show ap config 802.11a
- config 802.11b txPower
- config country

Config 802.11b Commands

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

config 802.11b 11gSupport

After enabling the Cisco wireless LAN solution 802.11b network using the **config 802.11b enable command**, enable or disable the Cisco wireless LAN solution 802.11g network using the **config 802.11b 11gSupport command**. Note that you must use this command to enable the network after configuring other 802.11b parameters.

Note that this command only enables the Cisco wireless LAN solution 802.11g network after the Cisco wireless LAN solution 802.11b network is enabled using the config 802.11b enable command. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual wireless LAN, use the **config wlan radio** command.

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

```
config 802.11b 11gSupport {enable | disable}
```

Syntax Description

config	Configure parameters.
802.11b	802.11b network parameters.
11gSupport	Support for the 802.11g network.
{enable disable}	Enable or disable 802.11g.

Defaults

Enabled.

Examples

```
> config 802.11b 11gSupport enable
```

```
Changing the 11gSupport will cause all the APs to reboot when you enable 802.11b network.
Are you sure you want to continue? (y/n) n
```

```
11gSupport not changed!
```

Related Commands

```
show sysinfo
show 802.11b
config 802.11b enable
config wlan radio
config 802.11b disable
config 802.11a disable
config 802.11a enable
```

config 802.11b antenna diversity

To configure the diversity option for 802.11b antennas, use the **config 802.11b antenna diversity** command.

config 802.11b antenna diversity {enable | sideA | sideB} Cisco_AP

Syntax Description		
config		Configure parameters.
802.11b antenna diversity		Diversity antennas for 802.11b/g.
enable		Between the two internal antennas.
sideA		Between the internal antennas and an external antenna connected to the Cisco lightweight access point Left port.
sideB		Between the internal antennas and an external antenna connected to the Cisco lightweight access point Right port.
<i>Cisco_AP</i>		Cisco lightweight access point name.

Defaults None.

Examples

To enable diversity for AP01:

```
> config 802.11b antenna diversity enable AP01
```

To enable diversity for AP01 using an external antenna connected to the Cisco lightweight access point Left port (sideA):

```
> config 802.11b antenna diversity sideA AP01
```

Related Commands

show ap config 802.11b
 config 802.11b disable
 config 802.11b enable
 config 802.11b extAntGain
 config 802.11b selection

config 802.11b antenna extAntGain

To configure the 802.11b/g external antenna gain, use the **config 802.11b antenna extAntGain** command.

Use the **config 802.11b disable** command to disable the 802.11b/g Cisco radio before using the **config 802.11b antenna extAntGain** command. After configuring the external antenna gain, use the **config 802.11b enable** command to enable the 802.11b/g Cisco radio.

config 802.11b antenna extAntGain *antenna_gain* *Cisco_AP*

Syntax Description	config	Configure parameters.
	802.11b antenna	Antennas for 802.11b/g Cisco radio.
	extAntGain	Configure external antenna gain.
	antenna_gain	Enter antenna gain in 0.5 dBm units (for example, 2.5 dBm = 5).
	Cisco_AP	Cisco lightweight access point name.

Defaults None.

Usage Guidelines

Before using the **config 802.11b antenna extAntGain** command, disable the 802.11b/g Cisco radio with the **config 802.11b disable** command.

After configuring the external antenna gain, use the **config 802.11b enable** command to enable the 802.11b/g Cisco radio.

Examples

To configure the 802.11b/g external antenna gain for AP1:

```
> config 802.11b antenna extAntGain 1 AP1
```

Related Commands

- config 802.11b disable
- config 802.11b enable
- config 802.11b diversity
- config 802.11b selection

config 802.11b antenna selection

To configure the 802.11b/g antenna selection (internal or external), use the **config 802.11b antenna selection** command.

config 802.11b antenna selection {internal | external} *Cisco_AP*

Syntax Description		
config		Configure parameters.
802.11b antenna selection		Antenna selection (internal or external) for 802.11b.
internal		Select internal antennas.
external		Select external antenna.
<i>Cisco_AP</i>		Cisco lightweight access point name.

Defaults None.

Examples > **config 802.11b antenna selection internal AP02**

Related Commands

- show ap config 802.11b
- config 802.11b disable
- config 802.11b enable
- config 802.11b extAntGain
- config 802.11b diversity

config 802.11b beaconperiod

In Cisco wireless LAN solution 802.11b/g networks, all Cisco lightweight access point wireless LANs broadcast a beacon at regular intervals. This beacon notifies clients that 802.11b/g service is available, and allows the clients to synchronize with the Cisco lightweight access point. To change the 802.11b/g beacon period for the whole 802.11b/g network, use the **config 802.11b beaconperiod** command.

Before you change the beacon period using the config 802.11b beaconperiod command, make sure that you have disabled the 802.11b/g network using the config 802.11b disable command. When you are done changing the beacon period, remember to enable the 802.11b/g network using the config 802.11b enable command.

config 802.11b beaconperiod *time_units*

Syntax Description	config	Configure parameters.
	802.11b	802.11b/g network parameters.
	beaconperiod	Send a beacon every 20 to 1000 milliseconds.
	<i>time_units</i>	Beacon interval (20–1000) in time units (TUs). One TU is 1024 micro seconds.

Defaults 100

Examples To configure an 802.11b/g network for a beacon period of 180 time units:
> **config 802.11b beaconperiod 180**

Related Commands

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

config 802.11b channel

To configure an 802.11b network or a single access point for automatic or manual channel selection, use the **config 802.11b channel** command.

```
config 802.11b channel { global [ auto | once | off ] } |
{AP ap_name [ global | channel ] }
```

When configuring 802.11b channels for a single lightweight access point, use the **config 802.11b disable** command to disable the 802.11b network. Then use the **config 802.11b channel** command to set automatic channel selection by Radio Resource Management (RRM) or manually set the channel for the 802.11b radio. Then enable the 802.11b network using the **config 802.11b enable** command.



Note

Refer to the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the channels supported by your access point. The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

Syntax Description

global	Configures the 802.11b operating channel for all lightweight access points.
auto	Specifies the channel is automatically set by radio resource management (RRM) for the 802.11b radio.
once	Specifies the channel is automatically set once by RRM.
off	Specifies the automatic channel selection by RRM is disabled.
ap	Configures the 802.11b operating channel for a specified lightweight access point.
<i>ap_name</i>	Specifies the access point name.
global	Specifies the 802.11b operating channel is automatically set by RRM and over-rides the existing configuration setting.
<i>channel</i>	Specifies a manual channel number to be used by the access point. The supported channels depend on the specific access point used and the regulatory region.

Defaults

This command has no defaults.

Examples

To configure all 802.11b channels for automatic channel configuration by the RRM based on availability and interference, use this command:

```
> config 802.11b channel global auto
```

To have RRM automatically reconfigure all 802.11b channels one time based on availability and interference, use this command:

```
> config 802.11b channel global once
```

To turn 802.11b automatic channel configuration off, use this command:

```
> config 802.11b channel global off
```

To configure all 802.11b channels in access point AP01 for automatic channel configuration, use this command:

```
> config 802.11b channel AP01 global
```

Related Commands

show 802.11b

config 802.11b disable

config 802.11b enable

config 802.11a channel

config country

config 802.11b disable

Disable or enable 802.11b/g transmissions for the whole network or for an individual Cisco radio using the **config 802.11b disable** command.

Note that you must use this command to disable the network before using other config 802.11b commands.

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

config 802.11b disable {network | Cisco_AP}

Syntax Description	
config	Configure parameters.
802.11b	802.11b/g network parameters.
disable	Disable 802.11b/g.
network	Whole network.
<i>Cisco_AP</i>	Override the network setting for an individual Cisco lightweight access point radio.

Defaults Enabled.

Examples

To disable the whole 802.11b/g network:

```
> config 802.11b disable network
```

To disable AP01 802.11b/g transmissions:

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

Related Commands

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

config 802.11b dtpc

To configure the 802.11b DTPC setting, use the **config 802.11b dtpc** command.

config 802.11b dtpc {enable | disable}

Syntax Description	config	Configure parameters.
	802.11b	802.11b network parameters.
	dtpc	Dynamic Transmit Power Control.
	{enable disable}	- Enter enable to enable DTPC setting configuration. - Enter disable to disable DTPC setting configuration.

Defaults	Enabled by default.

Examples	> config 802.11b dtpc disable

Related Commands	show 802.11b config 802.11b beaconperiod config 802.11b disable config 802.11b enable

config 802.11b enable

Note that you must use this command to enable the network after configuring other 802.11b parameters.

Note that this command only enables the Cisco wireless LAN solution 802.11b network. To enable the Cisco wireless LAN solution 802.11g network, you **MUST** have the 802.11b network enabled, and then **use the config 802.11b 11gSupport enable** command. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual wireless LAN, use the **config wlan radio** command.

This command can be used any time the CLI interface is active. Note that you must reboot the Cisco Wireless LAN controller to implement this command.

config 802.11b enable network

config 802.11b enable *Cisco_AP*

Syntax Description

config	Configure parameters.
802.11b	802.11b network parameters.
enable	Enable or disable 802.11b. Allow support for 802.11g.
network	For the whole network.
<i>Cisco_AP</i>	To override the network setting for individual Cisco lightweight access point radio.

Defaults

Enabled.

Examples

To enable the whole 802.11b network and provide support for the 802.11g network:

```
> config 802.11b enable network
```

To enable AP1 802.11b transmissions and support AP1 802.11g transmissions:

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

Related Commands

show sysinfo
show 802.11b
config 802.11b 11gSupport
config wlan radio
config 802.11b disable
config 802.11a disable
config 802.11a enable

config 802.11b exp-bwreq

To configure the CCX version 5 expedited bandwidth request feature for the 802.11b radio, use the **config 802.11b exp-bwreq** command. When this command is enabled, the controller configures all joining access points for this feature.

config 802.11b exp-bwreq [enable | disable]

Syntax Description

enable	Enables the expedited bandwidth request feature.
disable	Configures the mean datarate of a voice stream.

Defaults

The expedited bandwidth request feature is disabled by default.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> config 802.11b exp-bwreq enable
```

Cannot change Exp Bw Req mode while 802.11b network is opeational.

```
> config 802.11b disable network
> config 802.11b exp-bwreq enable
> config 802.11b enable network
```

Related Commands

```
show 802.11a
show ap stats 802.11a
```


config 802.11b fragmentation

To configure the 802.11b/g fragmentation threshold, use the **config 802.11b fragmentation** command. This command can only be used when the network is not operational.

config 802.11b fragmentation *threshold*

Syntax Description	config	Configure parameters.
	802.11b	802.11b network parameters.
	fragmentation	Fragmentation threshold.
	<i>threshold</i>	Fragmentation threshold value.

Defaults	None.

Examples	> config 802.11b fragmentation 6500

Related Commands	config 802.11a fragmentation show 802.11a, show auto-rft

config 802.11b pico-cell

To enable or disable the 802.11b/g pico-cell extensions, use the **config 802.11b pico-cell** command. This command can only be used when the network is not operational.

config 802.11b pico-cell {enable | disable}

Syntax Description	config	Configure parameters.
	802.11b	802.11b network parameters.
	pico-cell	Pico cell extensions.
	{enable disable}	Enable or disable.

Defaults	None.

Examples	> config 802.11b pico-cell enable

Related Commands	config 802.11a pico-cell show 802.11b

config 802.11b preamble

Use this command 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). This command can be used any time the CLI interface is active.

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



Note

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

config 802.11b preamble {long | short}

Syntax Description

config	Configure parameters.
802.11b	802.11b network parameters.
preamble	As defined in subclause 18.2.2.2.
{long short}	Long or short 802.11b preamble.

Defaults

Short.

Examples

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

> show 802.11b

Short Preamble mandatory..... Enabled

> config 802.11b preamble long
>(reset system with save)

> show 802.11b

Short Preamble mandatory..... Disabled
```

Related Commands

show 802.11b

config 802.11b rate

To configure 802.11b/g mandatory and supported operational rates, use the **config 802.11b rate** command.

config 802.11b rate {disabled | mandatory | supported} rate

The data rates set here are negotiated between the client and the Cisco Wireless LAN controller. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Cisco Wireless LAN controller, any associated client that also supports that rate may communicate with the Cisco lightweight access point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate.

Syntax Description

config	Configure parameters.
802.11b	802.11b/g network parameters.
rate	Configure mandatory and supported operational rates.
{disabled mandatory supported}	- Enter disabled to disable a rate. - Enter mandatory to set a rate to mandatory. - Enter supported to set a rate to supported.
<i>rate</i>	1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, or 54 Mbps data rate.

Defaults

None.

Examples

To set 802.11b/g transmission at a mandatory rate at 5.5 Mbps:
> **config 802.11b rate mandatory 5.5**

Related Commands

show ap config 802.11b, config 802.11a rate

config 802.11b txPower

To configure the 802.11b transmit power level for an automatic or a manual setting for all access points or a single access point, use the **config 802.11b txPower** command.

```
config 802.11b txPower { global [ auto | once | power_level ] } |
{ ap ap_name [ global | power_level ] }
```



Note

Refer to the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the maximum transmit power limits for your access point. The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

Syntax Description

global	Configures the 802.11b transmit power level for all lightweight access points.
auto	Specifies the power level is automatically set by radio resource management (RRM) for the 802.11b radio.
once	Specifies the power level is automatically set once by RRM.
<i>power_level</i>	Specifies the transmit power level number. The supported power levels depends on the specific access point used and the regulatory region. For example, the 1240 series access point supports 8 levels and the 1200 series access point supports 6 levels.
ap	Configures the 802.11b transmit power level for a specified lightweight access point.
<i>ap_name</i>	Specifies the access point name.
global	Specifies the 802.11b transmit power level is automatically set by RRM and over-rides the existing configuration setting.
<i>power_level</i>	Specifies a manual transmit power level number to be used by the access point. The supported power levels depends on the specific access point used and the regulatory region. For example, the 1240 series access point supports 8 levels and the 1200 series access point supports 6 levels.

Defaults

The command default (global, auto) is for automatic configuration by RRM.

Examples

To have RRM automatically set the transmit power for all 802.11b radios in all lightweight access points, use this command:

```
> config 802.11b txPower global auto
```

To manually set the 802.11b radio transmit power to level 5 for all lightweight access points, use this command:

```
> config 802.11b txPower global 5
```

To have RRM automatically set the 802.11b radio transmit power for access point AP1, use this command:

```
> config 802.11b txPower AP1 global
```

To manually set the 802.11b radio transmit power to power level 2 for access point AP1, use this command:

```
> config 802.11b txPower AP1 global
```

To set transmit power for 802.11b/g AP1 to power level 2:

```
> config 802.11b txPower AP1 2
```

Related Commands

show ap config 802.11b

config 802.11a txPower

config country

config 802.11h channelswitch

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

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

Syntax Description	config	Configure parameters.
	802.11h	802.11h network parameters.
	channelswitch	802.11h channel switch announcement.
	{ enable disable }	Enable or disable 802.11h channel switch announcement.
	<i>mode</i>	802.11h channel switch announcement mode.
	<i>value</i>	802.11h channel announcement value.

Defaults None.

Examples

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

Related Commands **show 802.11h**

config 802.11h powerconstraint

To configure 802.11h power constraint value, use the **config 802.11h powerconstraint** command.

config 802.11h powerconstraint *value*

Syntax Description	config	Configure parameters.
	802.11b	802.11h network parameters.
	<i>value</i>	802.11h power constraint value.

Defaults	None.

Examples	> config 802.11h powerconstraint 5

Related Commands	show 802.11h

config 802.11h setchannel

To configure a new channel using 802.11h channel announcement, use the **config 802.11h setchannel** command.

config 802.11h setchannel *Cisco_AP*

Syntax Description	config	Configure parameters.
	802.11h	802.11h network parameters.
	<i>Cisco_AP</i>	Cisco lightweight access point name.

Defaults	None.

Examples	> config 802.11h setchannel ap02

Related Commands	show 802.11h

config aaa auth

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

```
config aaa auth mgmt [ aaa_server_type] [aaa_server_type]
```

Syntax Description	mgmt	Configures the AAA authentication search order for controller management users by specifying up to three AAA authentication server types . The order the server types are entered specifies the AAA authentication search order.
	aaa_server_type	(Optional) Specifies the AAA authentication server type (local , radius , or tacacs). The local setting specifies the local database, the radius setting specifies the RADIUS server, and the tacacs setting specifies the TACACS+ server.

Defaults This command has no defaults.

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

Examples > config aaa auth mgmt radius local

Related Commands [show aaa auth](#)

config aaa auth mgmt

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

config aaa auth mgmt [radius | tacacs]

Syntax Description	mgmt	Configure the order of authentication when multiple databases are configured
	[radius tacacs]	(Optional) Enter radius to configure the order of authentication for radius servers. (Optional) Enter tacacs to configure the order of authentication for tacacs servers.

Defaults

This command has no defaults.

Examples

```
> config aaa auth mgmt radius
> config aaa auth mgmt tacacs
```

Related Commands

show aaa auth order

config acl apply

To apply the Access Control List (ACL) to the data path, use the **config acl apply** command.

config acl apply *rule_name*



Note

For a Cisco 2100 series wireless LAN controller, you must configure a pre-authentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any pre-authentication ACL for Cisco 4400 series wireless LAN controllers.

Syntax Description

config acl	Command action.
apply	Applies the ACL (name with up to 32 alphanumeric characters) to the data path.
<i>rule_name</i>	ACL name up to 32 alphanumeric characters.

Defaults

None.

Examples

> **config acl apply** ac101

Related Commands

show acl

config acl counter

To see if packets are hitting any of the ACLs configured on your controller, use the **config acl counter** command.

config acl counter {start | stop}



Note

ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

Syntax Description

config acl	Command action.
counter {start stop}	Enables or disables ACL counters for your controller.

Defaults

config acl counter stop

Examples

```
> config acl counter start
```

Related Commands

clear acl counters
show acl detailed

config acl create

To create a new ACL, use the **config acl create** command.

config acl create *rule_name*



Note For a Cisco 2100 series wireless LAN controller, you must configure a pre-authentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any pre-authentication ACL for Cisco 4400 series wireless LAN controllers.

Syntax Description	config acl	Command action.
	create	Create a new ACL.
	<i>rule_name</i>	ACL name up to 32 alphanumeric characters.

Defaults	None.

Examples	> config acl create ac101

Related Commands	show acl

config acl cpu

To create a new ACL rule that restricts the traffic reaching the CPU, use the **config acl cpu** command. This allows you to control the type of packets reaching the CPU.

config acl cpu rule_name {wired | wireless | both}

Syntax Description

config acl cpu	Command action.
None	Disable the CPU ACL.
<i>rule_name</i>	ACL name up to 32 alphanumeric characters.
wired	Enable ACL on wired traffic.
wireless	Enable ACL on wireless traffic
both	Enable ACL on both wired and wireless traffic.

Defaults

None.

Examples

The following example shows how to create an ACL named acl101 on the CPU and apply it to wired traffic.

```
> config acl cpu acl101 wired
```

Related Commands

[show acl cpu](#)

config acl delete

To delete an ACL, use the **config acl delete** command.

config acl delete *rule_name*



Note For a Cisco 2100 series wireless LAN controller, you must configure a pre-authentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any pre-authentication ACL for Cisco 4400 series wireless LAN controllers.

Syntax Description	config acl	Command action.
	delete	Delete an ACL.
	<i>rule_name</i>	ACL name up to 32 alphanumeric characters.

Defaults	None.

Examples	> config acl delete ac101

Related Commands	show acl

config acl rule

To configure ACL rules, use the **config acl rule** command.

```
config acl rule {
  action rule_name rule_index {permit | deny} |
  add rule_name rule_index |
  change index rule_name old_index new_index |
  delete rule_name rule_index |
  destination address rule_name rule_index ip_address netmask |
  destination port range rule_name rule_index start_port end_port |
  direction rule_name rule_index {in | out | any} |
  dscp rule_name rule_index dscp |
  protocol rule_name rule_index protocol |
  source address rule_name rule_index ip_address netmask |
  source port range rule_name rule_index start_port end_port |
  swap index rule_name index_1 index_2}
```



Note

For a Cisco 2100 series wireless LAN controller, you must configure a pre-authentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any pre-authentication ACL for Cisco 4400 series wireless LAN controllers.

Syntax Description

config acl	Command action.
rule	Configures ACL rules.
action	Configures a rule's action whether to permit or deny access.
add	Adds a new rule.
change	Changes a rule's index.
delete	Deletes a rule.
destination address	Configures a rule's destination IP address and netmask.
destination port range	Configures a rule's destination port range.
direction	Configures a rule's direction to in, out, or any.
dscp	Configures a rule's DSCP.
protocol	Configures a rule's IP Protocol.
source address	Configures a rule's source IP address, netmask.
source port range	Configures a rule's source port range.
swap	Swaps two rules' indices.
<i>rule_name</i>	ACL name up to 32 alphanumeric characters.
<i>rule_index</i>	Rule index between 1 and 32.
<i>ip_address</i>	The rule's IP Address.
<i>netmask</i>	The rule's netmask.
<i>start_port</i>	The start port number (between 0 and 65535).
<i>end_port</i>	The end port number (between 0 and 65535).

<i>dscp</i>	A number between 0 and 63, or any .
<i>protocol</i>	A number between 0 and 255, or any .

Defaults None.

Examples > config acl rule action lab1 4 permit

Related Commands show acl

Configure Advanced 802.11a Commands

Use the **advanced 802.11a** commands to configure advanced 802.11a settings.

config advanced 802.11a channel dca anchor-time

To specify the time of day when the DCA algorithm is to start, use the **config advanced 802.11a channel dca anchor-time** command.

config advanced 802.11a channel dca anchor-time *value*

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	channel	RRM channel selections.
	dca	Dynamic channel assignment.
	anchor-time	Time when DCA algorithm starts.
	<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

```
> config advanced 802.11a channel dca anchor-time 17
```

Related Commands

[config advanced 802.11a channel dca interval](#)
[config advanced 802.11a channel dca sensitivity](#)
[show advanced 802.11a channel](#)

config advanced 802.11a channel dca chan-width-11n

To configure the DCA channel width for all 802.11n radios in the 5-GHz band, use this command.

config advanced 802.11a channel dca chan-width-11n {20 | 40}

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
channel	RRM channel selections.
dca	Dynamic channel assignment.
chan-width-11n	Channel width for all 802.11n radios.
20	Sets the channel width for 802.11n radios to 20 MHz.
40	Sets the channel width for 802.11n radios to 40 MHz.

Defaults

Channel width is **20**.

Usage Guidelines

If you choose 40, be sure to set at least two adjacent channels in the **config advanced 802.11a 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 {802.11a | 802.11b} chan_width** command. If you ever then change the static configuration to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

Examples

```
> config advanced 802.11a channel dca chan-width-11n 40
```

Related Commands

config {802.11a | 802.11b} chan_width
config advanced 802.11a channel dca interval
config advanced 802.11a channel dca sensitivity
show advanced 802.11a channel

config advanced 802.11a channel dca interval

To specify how often the DCA algorithm is allowed to run, use the **config advanced 802.11a channel dca interval** command.

config advanced 802.11a channel dca interval *value*

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	channel	RRM channel selections.
	dca	Dynamic channel assignment.
	interval	How often the DCA algorithm is allowed to run.
	<i>value</i>	Valid values are 0, 1, 2, 3, 4, 6, 8, 12, or 24 hours. 0 is 10 minutes (600 seconds).

Defaults 0 (10 minutes).

Examples > **config advanced 802.11a channel dca interval 8**

Related Commands [config advanced 802.11a channel dca anchor-time](#)
[config advanced 802.11a channel dca sensitivity](#)
[show advanced 802.11a channel](#)

config advanced 802.11a channel dca sensitivity

To specify how sensitive the DCA algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels, use the **config advanced 802.11a channel dca sensitivity** command.

config advanced 802.11a channel dca sensitivity {low | medium | high}

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
channel	RRM channel selections.
dca	Dynamic channel assignment.
sensitivity	DCA algorithm sensitivity.
low	DCA algorithm is not particularly sensitive to environmental changes. See the “Usage Guidelines” section for more information.
medium	DCA algorithm is moderately sensitive to environmental changes. See the “Usage Guidelines” section for more information.
high	DCA algorithm is highly sensitive to environmental changes. See the “Usage Guidelines” section for more information.

Defaults

None.

Usage Guidelines

The DCA sensitivity thresholds vary by radio band, as noted below:

	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

Examples

```
> config advanced 802.11a channel dca sensitivity low
```

Related Commands

[config advanced 802.11a channel dca anchor-time](#)
[config advanced 802.11a channel dca interval](#)
[show advanced 802.11a channel](#)

config advanced 802.11a channel foreign

To have RRM consider or ignore foreign 802.11a interference avoidance in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11a channel foreign** command.

config advanced 802.11a channel foreign {enable | disable}

Syntax Description	
config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
channel	RRM channel selections.
foreign	Foreign interference.
{enable disable}	Enable foreign access point 802.11a interference avoidance in the channel assignment.
	Disable foreign access point 802.11a interference avoidance in the channel assignment.

Defaults Enabled.

Examples To have RRM consider foreign 802.11a interference when making channel selection updates for all 802.11a Cisco lightweight access points:

```
> config advanced 802.11a channel foreign enable
```

Related Commands

show advanced 802.11a channel

config advanced 802.11b channel foreign

config advanced 802.11a channel load

To have RRM consider or ignore traffic load in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11a channel load** command.

```
config advanced 802.11a channel load {enable | disable}
```

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	channel	RRM channel selections.
	load	Traffic load.
	{enable disable}	Enable the Cisco lightweight access point 802.11a load avoidance in the channel assignment. Disable the Cisco lightweight access point 802.11a load avoidance in the channel assignment.

Defaults Disabled.

Examples To have RRM consider traffic load when making channel selection updates for all 802.11a Cisco lightweight access points:

```
> config advanced 802.11a channel load enable
```

Related Commands

show advanced 802.11a channel

config advanced 802.11b channel load

config advanced 802.11a channel noise

To have RRM consider or ignore non-802.11a noise in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11a channel noise** command.

config advanced 802.11a channel noise {enable | disable}

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
channel	RRM channel selections.
noise	Non-802.11a noise.
{enable disable}	Enable non-802.11a noise avoidance in the channel assignment. or ignore. Disable non-802.11a noise avoidance in the channel assignment.

Defaults

Disabled.

Examples

To have RRM consider non-802.11a noise when making channel selection updates for all 802.11a Cisco lightweight access points:

```
> config advanced 802.11a channel noise enable
```

Related Commands

show advanced 802.11a channel
config advanced 802.11b channel noise

config advanced 802.11a channel update

To have RRM initiate a channel selection update for all 802.11a Cisco lightweight access points, use the **config advanced 802.11a channel update** command.

config advanced 802.11a channel update

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	channel update	Have RRM update the channel selections.

Defaults None.

Examples > **config advanced 802.11a channel update**

Related Commands **show advanced 802.11a channel**
 config advanced 802.11b channel update

config advanced 802.11a coverage

To enable or disable coverage hole detection, use the **config advanced 802.11a coverage** command.

config advanced 802.11a coverage {enable | disable}

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	coverage	Coverage hole detection.
	enable	Enable coverage hole detection.
	disable	Disable coverage hole detection.

Defaults Enabled.

Usage Guidelines

If you enable coverage hole detection, the controller automatically determines, based on data that is received from the access points, whether any access points have clients that are potentially located in areas with poor coverage.

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11a coverage packet-count** and **config advanced 802.11a 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 802.11a coverage level global** and **config advanced 802.11a coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11a coverage enable
```

Related Commands

- config advanced 802.11a coverage exception global**
- config advanced 802.11a coverage fail-rate**
- config advanced 802.11a coverage level global**
- config advanced 802.11a coverage packet-count**
- config advanced 802.11a coverage rssi-threshold**
- show advanced 802.11a coverage**

config advanced 802.11a 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 802.11a coverage exception global** command.

config advanced 802.11a coverage exception global *percent*

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
coverage	Coverage hole detection.
exception	Specifies the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point.
global	Specifies the parameter for all 802.11a access points.
<i>percent</i>	Percentage of clients. Valid values are from 0 to 100%.

Defaults

25%.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11a coverage packet-count** and **config advanced 802.11a 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 802.11a coverage level global** and **config advanced 802.11a coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11a coverage exception global 50
```

Related Commands

config advanced 802.11a coverage
config advanced 802.11a coverage fail-rate
config advanced 802.11a coverage level global
config advanced 802.11a coverage packet-count
config advanced 802.11a coverage rssi-threshold
show advanced 802.11a coverage

config advanced 802.11a coverage fail-rate

To specify the failure rate threshold for uplink data or voice packets, use the **config advanced 802.11a coverage fail-rate** command.

config advanced 802.11a coverage {data | voice} fail-rate *percent*

Syntax Description		
config		Configure parameters.
advanced 802.11a		Advanced 802.11a parameters.
coverage		Coverage hole detection.
data		Specifies threshold for data packets.
voice		Specifies threshold for voice packets.
fail-rate		Configures the threshold count for minimum uplink failures for data or voice packets.
<i>percent</i>		The failure rate as a percentage. Valid values are from 1 to 100 percent.

Defaults 20.

Usage Guidelines If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11a coverage packet-count** and **config advanced 802.11a 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 802.11a coverage level global** and **config advanced 802.11a coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples > **config advanced 802.11a coverage data fail-rate 80**

Related Commands

- config advanced 802.11a coverage**
- config advanced 802.11a coverage exception global**
- config advanced 802.11a coverage level global**
- config advanced 802.11a coverage packet-count**
- config advanced 802.11a coverage rssi-threshold**
- show advanced 802.11a coverage**

config advanced 802.11a coverage level global

To specify the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold, use the **config advanced 802.11a coverage level global** command.

config advanced 802.11a coverage level global *clients*

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
coverage	Coverage hole detection.
level	Specifies the minimum number of clients on an access point with an RSSI value at or below the RSSI threshold.
global	Specifies the parameter for all 802.11a access points.
<i>clients</i>	Minimum number of clients. Valid values are from 1 to 75.

Defaults

3.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11a coverage packet-count** and **config advanced 802.11a 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 802.11a coverage level global** and **config advanced 802.11a coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11a coverage level global 60
```

Related Commands

config advanced 802.11a coverage
config advanced 802.11a coverage exception global
config advanced 802.11a coverage fail-rate
config advanced 802.11a coverage packet-count
config advanced 802.11a coverage rssi-threshold
show advanced 802.11a coverage

config advanced 802.11a coverage packet-count

To specify the minimum failure count threshold for uplink data or voice packets, use the **config advanced 802.11a coverage packet-count** command.

config advanced 802.11a coverage {data | voice} packet-count *packets*

Syntax Description		
config		Configure parameters.
advanced 802.11a		Advanced 802.11a parameters.
coverage		Coverage hole detection.
data		Specifies threshold for data packets.
voice		Specifies threshold for voice packets.
packet-count		Configures the threshold count for minimum uplink failures for data or voice packets.
<i>packets</i>		Minimum number of packets. Valid values are from 1 to 255 packets.

Defaults 10.

Usage Guidelines If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11a coverage packet-count** and **config advanced 802.11a 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 802.11a coverage level global** and **config advanced 802.11a coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples > **config advanced 802.11a coverage data packet-count 100**

Related Commands

- config advanced 802.11a coverage**
- config advanced 802.11a coverage exception global**
- config advanced 802.11a coverage fail-rate**
- config advanced 802.11a coverage level global**
- config advanced 802.11a coverage rssi-threshold**
- show advanced 802.11a coverage**

config advanced 802.11a 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 802.11a coverage rssi-threshold** command.

config advanced 802.11a coverage {data | voice} rssi-threshold *rssi*

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
coverage	Coverage hole detection.
data	Specifies threshold for data packets.
voice	Specifies threshold for voice packets.
rssi-threshold	Receive signal strength indication threshold.
<i>rssi</i>	Valid values are from –60 to –90 dBm.

Defaults

- Data packets: –80 dBm.
- Voice packets: –75 dBm.

Usage Guidelines

The *rssi* value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data or voice queue with an RSSI value that is below the value that you enter here, a potential coverage hole has been detected.

The access point takes RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11a coverage packet-count** and **config advanced 802.11a 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 802.11a coverage level global** and **config advanced 802.11a coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11a coverage data rssi-threshold -60
```

Related Commands

config advanced 802.11a coverage
config advanced 802.11a coverage exception global
config advanced 802.11a coverage fail-rate
config advanced 802.11a coverage level global
config advanced 802.11a coverage packet-count
show advanced 802.11a coverage

config advanced 802.11a edca-parameters

To enable a specific enhanced distributed channel access (EDCA) profile on the 802.11a network, use the **config advanced 802.11a edca-parameters** command.

```
config advanced 802.11a edca-parameters { wmm-default | svp-voice | optimized-voice |
optimized-video-voice }
```

Syntax Description		
config		Configure parameters.
advanced 802.11a		Advanced 802.11a parameters.
edca-parameters		Enables a specific EDCA profile.
wmm-default		Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network.
svp-voice		Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls.
optimized-voice		Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network.
optimized-video-voice		Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
	Note	If you deploy video services, admission control (ACM) must be disabled.

Defaults

wmm-default

Examples

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

Related Commands

show 802.11a
config advanced 802.11b edca-parameters

config advanced 802.11a factory

To reset 802.11a advanced settings back to the factory defaults, use the **config advanced 802.11a factory** command.

config advanced 802.11a factory

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	factory	Return all 802.11a advanced settings to their factory defaults.

Defaults	None.

Examples	> config advanced 802.11a factory

Related Commands	show advanced 802.11a channel

config advanced 802.11a group-mode

To set the 802.11a automatic RF group selection mode on or off, use the **config advanced 802.11a group-mode** command.

config advanced 802.11a group-mode {auto | off}

Syntax Description		
config		Configure parameters.
advanced 802.11a		Advanced 802.11a parameters.
group-mode		Cisco radio RF grouping.
{ auto off }		Enter auto to set the 802.11a RF group selection to automatic update mode. Enter off to set the 802.11a RF group selection off.

Defaults Auto.

Examples

To turn the 802.11a automatic RF group selection mode on:

```
> config advanced 802.11a group-mode auto
```

To turn the 802.11a automatic RF group selection mode off:

```
> config advanced 802.11a group-mode off
```

Related Commands

show advanced 802.11a group
config advanced 802.11b group-mode

config advanced 802.11a logging channel

To turn the channel change logging mode on or off, use the **config advanced 802.11a logging channel** command.

config advanced 802.11a logging channel {on | off}

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
logging channel	Log channel changes.
{on off}	Enable or disable 802.11a channel logging.

Defaults

Off (disabled).

Examples

```
> config advanced 802.11a logging channel on
```

Related Commands

show advanced 802.11a logging
config advanced 802.11b logging channel

config advanced 802.11a logging coverage

To turn the coverage profile logging mode on or off, use the **config advanced 802.11a logging coverage** command.

config advanced 802.11a logging coverage {on | off}

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	logging coverage	Log coverage changes.
	{on off}	Enable or disable 802.11a coverage profile violation logging.

Defaults	Off (disabled).

Examples	> config advanced 802.11a logging coverage on

Related Commands	show advanced 802.11a logging config advanced 802.11b logging coverage

config advanced 802.11a logging foreign

To turn the foreign interference profile logging mode on or off, use the **config advanced 802.11a logging foreign** command.

config advanced 802.11a logging foreign {on | off}

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
logging foreign	Log foreign changes.
{on off}	Enable or disable 802.11a foreign interference profile violation logging.

Defaults

Off (disabled).

Examples

```
> config advanced 802.11a logging foreign on
```

Related Commands

show advanced 802.11a logging
config advanced 802.11b logging foreign

config advanced 802.11a logging load

To turn the 802.11a load profile logging mode on or off, use the **config advanced 802.11a logging load** command.

config advanced 802.11a logging load {on | off}

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	logging load	Log load changes.
	{on off}	Enable or disable 802.11a load profile violation logging.

Defaults Off (disabled).

Examples > **config advanced 802.11a logging load on**

Related Commands **show advanced 802.11a logging**
config advanced 802.11b logging load

config advanced 802.11a logging noise

To turn the 802.11a noise profile logging mode on or off, use the **config advanced 802.11a logging noise** command.

config advanced 802.11a logging noise {on | off}

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
logging noise	Log noise changes.
{on off}	Enable or disable 802.11a noise profile violation logging.

Defaults

Off (disabled).

Examples

```
> config advanced 802.11a logging noise on
```

Related Commands

show advanced 802.11a logging
config advanced 802.11b logging noise

config advanced 802.11a logging performance

To turn the 802.11a performance profile logging mode on or off, use the **config advanced 802.11a logging performance** command.

config advanced 802.11a logging performance {on | off}

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	logging performance	Log performance changes.
	{on off}	Enable or disable 802.11a performance profile violation logging.

Defaults Off (disabled).

Examples > **config advanced 802.11a logging performance on**

Related Commands **show advanced 802.11a logging**
config advanced 802.11b logging performance

config advanced 802.11a logging txpower

To turn the 802.11a transmit power change logging mode on or off, use the **config advanced 802.11a logging txpower** command.

config advanced 802.11a logging txpower {on | off}

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	logging txpower	Log power changes.
	{on off}	Enable or disable 802.11a transmit power change logging.

Defaults Off (disabled).

Examples > **config advanced 802.11a logging txpower off**

Related Commands show advanced 802.11a logging
config advanced 802.11b logging power

config advanced 802.11a monitor channel-list

To set the 802.11a noise, interference, and rogue monitoring channel list, use the **config advanced 802.11a monitor channel-list** command.

config advanced 802.11a monitor channel-list {all | country | dca}

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
monitor channel-list	Monitor coverage interval.
{all country dca}	- Enter all to monitor all channels. - Enter country to monitor the channels used in the configured country code. - Enter dca to monitor the channels used by the automatic channel assignment.

Defaults

country.

Examples

```
> config advanced 802.11a monitor channel-list country
```

Related Commands

show advanced 802.11a monitor coverage

config advanced 802.11a monitor coverage

To set the coverage measurement interval between 60 and 3600 seconds, use the **config advanced 802.11a monitor coverage** command.

config advanced 802.11a monitor coverage *seconds*

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
monitor coverage	Monitor coverage interval.
<i>seconds</i>	Coverage measurement interval between 60 and 3600 seconds.

Defaults

180 seconds.

Examples

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 802.11a monitor load

To set the load measurement interval between 60 and 3600 seconds, use the **config advanced 802.11a monitor load** command.

config advanced 802.11a monitor load *seconds*

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	monitor load	Monitor load interval.
	<i>seconds</i>	Load measurement interval between 60 and 3600 seconds.

Defaults	60 seconds.

Examples	To set the load measurement interval to 60 seconds: > config advanced 802.11a monitor load 60

Related Commands	show advanced 802.11a monitor config advanced 802.11b monitor load

config advanced 802.11a monitor mode

To enable or disable 802.11a access point monitoring, use the **config advanced 802.11a monitor mode** command.

```
config advanced 802.11a monitor mode {enable | disable}
```

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	monitor mode	Monitor mode.
	{enable disable}	Enable or disable 802.11a access point monitoring.

Defaults Enabled.

Examples > config advanced 802.11a monitor mode enable

Related Commands show advanced 802.11a monitor
config advanced 802.11b monitor mode

config advanced 802.11a monitor noise

To set the 802.11a noise measurement interval between 60 and 3600 seconds, use the **config advanced 802.11a monitor noise** command.

config advanced 802.11a monitor noise *seconds*

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	monitor noise	Monitor noise interval.
	<i>seconds</i>	Noise measurement interval between 60 and 3600 seconds.

Defaults	180 seconds.

Examples	To set the noise measurement interval to 120 seconds: > config advanced 802.11a monitor noise 120

Related Commands	show advanced 802.11a monitor config advanced 802.11b monitor noise

config advanced 802.11a monitor signal

To set the signal measurement interval between 60 and 3600 seconds, use the **config advanced 802.11a monitor signal** command.

config advanced 802.11a monitor signal *seconds*

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	monitor signal	Monitor signal interval.
	<i>seconds</i>	Signal measurement interval between 60 and 3600 seconds.

Defaults 60 seconds.

Examples To set the signal measurement interval to 120 seconds:
> **config advanced 802.11a monitor signal 120**

Related Commands **show advanced 802.11a monitor**
config advanced 802.11b monitor signal

config advanced 802.11a profile clients

To set the Cisco lightweight access point clients threshold between 1 and 75 clients, use the **config advanced 802.11a profile clients** command.

config advanced 802.11a profile clients {**global** | *Cisco_AP*} *clients*

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile clients	Cisco lightweight access point Client profile
	{ global <i>Cisco_AP</i> }	- Enter global to configure all 802.11a Cisco lightweight access points. - Enter a Cisco lightweight access point name.
	<i>clients</i>	802.11a Cisco lightweight access point client threshold between 1 and 75 clients.

Defaults 12 clients.

Examples To set all Cisco lightweight access point clients thresholds to 25 clients:

```
> config advanced 802.11a profile clients global 25
```

Global client count profile set.

To set the AP1 clients threshold to 75 clients:

```
> config advanced 802.11a profile clients AP1 75
```

Global client count profile set.

Related Commands

show advanced 802.11a profile

config advanced 802.11b profile clients

config advanced 802.11a profile customize

To turn customizing on or off for an 802.11a Cisco lightweight access point performance profile, use the **config advanced 802.11a profile customize** command.

```
config advanced 802.11a profile customize Cisco_AP {on | off}
```

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	customize	Performance profile.
	Cisco_AP	Cisco lightweight access point.
	{on off}	Enter on to customize performance profiles for this Cisco lightweight access point. Enter off to use global default performance profiles for this Cisco lightweight access point.

Defaults Off.

Examples To turn performance profile customization on for 802.11a Cisco lightweight access point AP1:
> config advanced 802.11a profile customize AP1 on

Related Commands show advanced 802.11a profile
config advanced 802.11b profile customize

config advanced 802.11a profile foreign

To set the foreign 802.11a transmitter interference threshold between 0 and 100 percent, use the **config advanced 802.11a profile foreign** command.

config advanced 802.11a profile foreign {**global** | *Cisco_AP*} *percent*

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile foreign	Foreign interference profile.
	{ global <i>Cisco_AP</i> }	Global or Cisco lightweight access point specific profile.
	<i>percent</i>	802.11a foreign 802.11a interference threshold between 0 and 100 percent.

Defaults 10.

Examples To set the Other 802.11a transmitter interference threshold for all Cisco lightweight access points to 50 percent:

```
> config advanced 802.11a profile foreign global 50
```

To set the Other 802.11a transmitter interference threshold for AP1 to 0 percent:

```
> config advanced 802.11a profile foreign AP1 0
```

Related Commands

show advanced 802.11a profile

config advanced 802.11b profile foreign

config advanced 802.11a profile noise

To set the 802.11a foreign noise threshold between -127 and 0 dBm, use the **config advanced 802.11a profile noise** command.

config advanced 802.11a profile noise {**global** | *Cisco_AP*} *dBm*

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
profile noise	Profile noise limits.
{ global <i>Cisco_AP</i> }	Global or Cisco lightweight access point specific profile.
<i>dBm</i>	802.11a foreign noise threshold between -127 and 0 dBm.

Defaults

-70 dBm.

Examples

To set the 802.11a foreign noise threshold for all Cisco lightweight access points to -127 dBm:

```
> config advanced 802.11a profile noise global -127
```

To set the 802.11a foreign noise threshold for AP1 to 0 dBm:

```
> config advanced 802.11a profile noise AP1 0
```

Related Commands

show advanced 802.11a profile

config advanced 802.11b profile noise

config advanced 802.11a profile throughput

To set the Cisco lightweight access point data-rate throughput threshold between 1000 and 10000000 bytes per second, use the **config advanced 802.11a profile throughput** command.

config advanced 802.11a profile throughput {*global* | *Cisco_AP*} *value*

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile throughput	Data rate threshold.
	{ <i>global</i> <i>Cisco_AP</i> }	Global or Cisco lightweight access point specific profile.
	<i>value</i>	802.11a Cisco lightweight access point throughput threshold between 1000 and 10000000 bytes per second.

Defaults 1,000,000 bytes per second.

Examples To set all Cisco lightweight access point data-rate thresholds to 1000 bytes per second:

```
> config advanced 802.11a profile data-rate global 1000
```

To set the AP1 data-rate threshold to 10000000 bytes per second:

```
> config advanced 802.11a profile data-rate AP1 10000000
```

Related Commands

show advanced 802.11a profile

config advanced 802.11b profile data-rate

config advanced 802.11a profile utilization

To set the RF utilization threshold between 0 and 100 percent, use the **config advanced 802.11a profile utilization** command. OS generates a trap when this threshold is exceeded.

config advanced 802.11a profile utilization {**global** | *Cisco_AP*} *percent*

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
profile utilization	Cisco lightweight access point profile utilization
{global Cisco_AP}	Global or Cisco lightweight access point specific profile.
<i>percent</i>	802.11a RF utilization threshold between 0 and 100 percent.

Defaults

80 percent.

Examples

To set the RF utilization threshold for all Cisco lightweight access points to 0 percent:

```
> config advanced 802.11a profile utilization global 0
```

To set the RF utilization threshold for AP1 to 100 percent:

```
> config advanced 802.11a profile utilization AP1 100
```

Related Commands

show advanced 802.11a profile

config advanced 802.11b profile utilization

config advanced 802.11a receiver

To set the advanced receiver configuration, use the **config advanced 802.11a receiver** command.

config advanced 802.11a receiver {**default** | **rxstart jumpThreshold** *value*}

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	receiver	Receiver configuration.
	default	Default advanced receiver configuration.
	rxstart jumpThreshold <i>value</i>	802.11a advanced receiver start signal jump threshold configuration value (between 0 and 127).

Defaults	None.

Examples	To prevent changes to receiver parameters while network is enabled: > config advanced802.11a receiver default

Related Commands	config advanced 802.11b receiver

config advanced 802.11a receiver pico-cell-V2

If pico cell mode version 2 is enabled, use the **config advanced 802.11a receiver pico-cell-V2** command to configure the receive sensitivity.

```
config advanced 802.11a receiver pico-cell-V2 {rx_sense_threshold | cca_sense_threshold |
sta_tx_pwr} min max current
```

Syntax Description		
config		Configure parameters.
advanced 802.11a		Advanced 802.11a parameters.
receiver		Receiver configuration.
pico-cell-V2		Pico cell version 2 parameters.
rx_sense_threshold		Configure the receive sensitivity threshold.
cca_sense_threshold		Configure the CCA sensitivity threshold.
sta_tx_pwr		To configure the transmit power.
<i>min max current</i>		Measured in dBm.

Defaults None.

Examples

```
> config advanced 802.11a receiver pico-cell-V2 rx_sense_threshold -127 127 10
> config advanced 802.11a receiver pico-cell-V2 cca_sense_threshold -127 127 10
> config advanced 802.11a receiver pico-cell-V2 sta_tx_power -127 127 -65
```

Related Commands

```
config advanced 802.11a receiver
config advanced 802.11a receiver pico-cell-V2 send_iapp_req client_mac
```


config advanced 802.11a receiver pico-cell-V2 send_iapp_req

If pico cell mode version 2 is enabled and you want to transmit a unicast IAPP high-density frame request to a specific client, enter this command:

config advanced 802.11a receiver pico-cell-V2 send_iapp_req *client_mac*

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11b parameters.
receiver	Receiver configuration.
pico-cell-V2	Pico cell version 2 parameters.
send_iapp_req	Send a unicast IAPP high-density frame request.
<i>client_mac</i>	Specify the client mac address.

Defaults

None.

Examples

```
> config advanced 802.11a receiver pico-cell-V2 send_iapp_req 10:2b:3c:4d:5e:62
```

Related Commands

config advanced 802.11a receiver

config advanced 802.11a receiver pico-cell-V2 {rx_sense_threshold | cca_sense_threshold | sta_tx_pwr} *min max current*

config advanced 802.11a txpower-update

To initiate updates of the 802.11a transmit power for every Cisco lightweight access point, use the **config advanced 802.11a txpower-update** command.

config advanced 802.11a txpower-update

Syntax Description	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	txpower-update	Update transmission power

Defaults None.

Examples > **config advanced 802.11a txpower-update**

Related Commands **config advance 802.11b txpower-update**

Configure Advanced 802.11b Commands

Use the **advanced 802.11b** commands to configure advanced 802.11b settings.

config advanced 802.11b 7920VSIEConfig

To configure the 7920 VISE parameters, use the **config advanced 802.11b 7920VSIEConfig** command.

```
config advanced 802.11b 7920VSIEConfig { call-admission-limit limit |
G711-CU-Quantum quantum }
```

Syntax Description	
config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
7920VSIEConfig	Configure 7920 VISE parameters.
{ call-admission-limit G711-CU-Quantum }	- Enter call-admission-limit to configure the call admission limit for the 7920s. - Enter G711-CU-Quantum to configure the value supplied by the infrastructure indicating the current number of channel utilization units which would be used by a single G.711-20ms call.
<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 > `config advanced 802.11b 7920VSIEConfig call-admission-limit 4`

Related Commands None.

config advanced 802.11b channel dca anchor-time

To specify the time of day when the DCA algorithm is to start, use the **config advanced 802.11b channel dca anchor-time** command.

config advanced 802.11b channel dca anchor-time *value*

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b parameters.
channel	RRM channel selections.
dca	Dynamic channel assignment.
anchor-time	Time when DCA algorithm starts.
<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

```
> config advanced 802.11b channel dca anchor-time 17
```

Related Commands

[config advanced 802.11b channel dca interval](#)
[config advanced 802.11b channel dca sensitivity](#)
[show advanced 802.11b channel](#)

config advanced 802.11b channel dca interval

To specify how often the DCA algorithm is allowed to run, use the **config advanced 802.11b channel dca interval** command.

config advanced 802.11b channel dca interval *value*

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b parameters.
	channel	RRM channel selections.
	dca	Dynamic channel assignment.
	interval	How often the DCA algorithm is allowed to run.
	<i>value</i>	Valid values are 0, 1, 2, 3, 4, 6, 8, 12, or 24 hours. 0 is 10 minutes (600 seconds).

Defaults 0 (10 minutes).

Examples > **config advanced 802.11b channel dca interval 6**

Related Commands [config advanced 802.11b channel dca anchor-time](#)
[config advanced 802.11b channel dca sensitivity](#)
[show advanced 802.11b channel](#)

config advanced 802.11b channel dca sensitivity

To specify how sensitive the DCA algorithm is to environmental changes (such as signal, load, noise, and interference) when determining whether or not to change channels, use the **config advanced 802.11b channel dca sensitivity** command.

config advanced 802.11b channel dca sensitivity {low | medium | high}

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b parameters.
channel	RRM channel selections.
dca	Dynamic channel assignment.
sensitivity	DCA algorithm sensitivity.
low	DCA algorithm is not particularly sensitive to environmental changes. See the “Usage Guidelines” section for more information.
medium	DCA algorithm is moderately sensitive to environmental changes. See the “Usage Guidelines” section for more information.
high	DCA algorithm is highly sensitive to environmental changes. See the “Usage Guidelines” section for more information.

Defaults

None.

Usage Guidelines

The DCA sensitivity thresholds vary by radio band, as noted below:

	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

Examples

```
> config advanced 802.11b channel dca anchor-time medium
```

Related Commands

[config advanced 802.11b channel dca anchor-time](#)
[config advanced 802.11b channel dca interval](#)
[show advanced 802.11b channel](#)

config advanced 802.11b channel foreign

To have RRM consider or ignore foreign 802.11b/g interference in making channel selection updates for all 802.11b/g Cisco lightweight access points, use the **config advanced 802.11b channel foreign** command.

config advanced 802.11b channel foreign {enable | disable}

Syntax Description		
	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	channel	RRM channel selections.
	foreign	Foreign interference.
	{enable disable}	Consider or ignore foreign access point 802.11b interference avoidance in the channel assignment.

Defaults Enabled.

Examples To have RRM consider foreign 802.11b/g interference when making channel selection updates for all 802.11b/g Cisco lightweight access points:

```
> config advanced 802.11b channel foreign enable
```

Related Commands

show advanced 802.11b channel

config advanced 802.11a channel foreign

config advanced 802.11b channel load

To have RRM consider or ignore traffic load in making channel selection updates for all 802.11b/g Cisco lightweight access points, use the **config advanced 802.11b channel load** command.

config advanced 802.11b channel load {enable | disable}

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	channel	RRM channel selections.
	load	Traffic load.
	{enable disable}	Consider or ignore access point 802.11b load avoidance in the channel assignment.

Defaults Disabled.

Examples To have RRM consider traffic load when making channel selection updates for all 802.11b/g Cisco lightweight access points:

```
> config advanced 802.11b channel load enable
```

Related Commands show advanced 802.11b channel
config advanced 802.11a channel load

config advanced 802.11b channel noise

To have RRM consider or ignore non-802.11b/g noise in making channel selection updates for all 802.11b/g Cisco lightweight access points, use the **config advanced 802.11b channel noise** command.

config advanced 802.11b channel noise {enable | disable}

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	channel	RRM channel selections.
	noise	Non-802.11b/g noise.
	{enable disable}	Consider or ignore non-802.11b/g noise avoidance in the channel assignment.

Defaults Disabled.

Examples To have RRM consider non-802.11b/g noise when making channel selection updates for all 802.11b/g Cisco lightweight access points:

```
> config advanced 802.11b channel noise enable
```

Related Commands

- show advanced 802.11b channel
- config advanced 802.11a channel noise

config advanced 802.11b channel update

To have RRM initiate a channel selection update for all 802.11b/g Cisco lightweight access points, use the **config advanced 802.11b channel update** command.

config advanced 802.11b channel update

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	channel update	Update the channel selections.

Defaults	None.

Examples	> config advanced 802.11b channel update

Related Commands	show advanced 802.11b channel config advanced 802.11a channel update

config advanced 802.11b coverage

To enable or disable coverage hole detection, use the **config advanced 802.11b coverage** command.

config advanced 802.11b coverage {enable | disable}

Syntax Description		
config		Configure parameters.
advanced 802.11b		Advanced 802.11b parameters.
coverage		Coverage hole detection.
enable		Enable coverage hole detection.
disable		Disable coverage hole detection.

Defaults Enabled.

Usage Guidelines If you enable coverage hole detection, the controller automatically determines, based on data that is received from the access points, if 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 802.11b coverage packet-count** and **config advanced 802.11b 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 802.11b coverage level global** and **config advanced 802.11b coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples > **config advanced 802.11b coverage disable**

Related Commands

- config advanced 802.11b coverage exception global**
- config advanced 802.11b coverage fail-rate**
- config advanced 802.11b coverage level global**
- config advanced 802.11b coverage packet-count**
- config advanced 802.11b coverage rssi-threshold**
- show advanced 802.11b coverage**

config advanced 802.11b 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 802.11b coverage exception global** command.

config advanced 802.11b coverage exception global *percent*

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b parameters.
coverage	Coverage hole detection.
exception	Specifies the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point.
global	Specifies the parameter for all 802.11b access points.
<i>percent</i>	Percentage of clients. Valid values are from 0 to 100%.

Defaults

25%.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11b coverage packet-count** and **config advanced 802.11b 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 802.11b coverage level global** and **config advanced 802.11b coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11b coverage exception global 60
```

Related Commands

config advanced 802.11b coverage
config advanced 802.11b coverage fail-rate
config advanced 802.11b coverage level global
config advanced 802.11b coverage packet-count
config advanced 802.11b coverage rssi-threshold
show advanced 802.11b coverage

config advanced 802.11b coverage fail-rate

To specify the failure rate threshold for uplink data or voice packets, use the **config advanced 802.11b coverage fail-rate** command.

config advanced 802.11b coverage {data | voice} fail-rate *percent*

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b parameters.
coverage	Coverage hole detection.
data	Specifies threshold for data packets.
voice	Specifies threshold for voice packets.
fail-rate	Configures the threshold count for minimum uplink failures for data or voice packets.
<i>percent</i>	The failure rate as a percentage. Valid values are from 1 to 100 percent.

Defaults

20.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11b coverage packet-count** and **config advanced 802.11b 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 802.11b coverage level global** and **config advanced 802.11b coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11b coverage data fail-rate 60
```

Related Commands

config advanced 802.11b coverage
config advanced 802.11b coverage exception global
config advanced 802.11b coverage level global
config advanced 802.11b coverage packet-count
config advanced 802.11b coverage rssi-threshold
show advanced 802.11b coverage

config advanced 802.11b coverage level global

To specify the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold, use the **config advanced 802.11b coverage level global** command.

config advanced 802.11b coverage level global *clients*

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b parameters.
coverage	Coverage hole detection.
level	Specifies the minimum number of clients on an access point with an RSSI value at or below the RSSI threshold.
global	Specifies the parameter for all 802.11b access points.
<i>clients</i>	Minimum number of clients. Valid values are from 1 to 75.

Defaults

3.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11b coverage packet-count** and **config advanced 802.11b 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 802.11b coverage level global** and **config advanced 802.11b coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11b coverage level global 60
```

Related Commands

config advanced 802.11b coverage
config advanced 802.11b coverage exception global
config advanced 802.11b coverage fail-rate
config advanced 802.11b coverage packet-count
config advanced 802.11b coverage rssi-threshold
show advanced 802.11b coverage

config advanced 802.11b coverage packet-count

To specify the minimum failure count threshold for uplink data or voice packets, use the **config advanced 802.11b coverage packet-count** command.

config advanced 802.11b coverage {data | voice} packet-count *packets*

Syntax Description		
config		Configure parameters.
advanced 802.11b		Advanced 802.11b parameters.
coverage		Coverage hole detection.
data		Specifies threshold for data packets.
voice		Specifies threshold for voice packets.
packet-count		Configures the threshold count for minimum uplink failures for data or voice packets.
<i>packets</i>		Minimum number of packets. Valid values are from 1 to 255 packets.

Defaults

10.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11b coverage packet-count** and **config advanced 802.11b 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 802.11b coverage level global** and **config advanced 802.11b coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11b coverage voice packet-count 70
```

Related Commands

config advanced 802.11b coverage
config advanced 802.11b coverage exception global
config advanced 802.11b coverage fail-rate
config advanced 802.11b coverage level global
config advanced 802.11b coverage rssi-threshold
show advanced 802.11b coverage

config advanced 802.11b 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 802.11b coverage rssi-threshold** command.

config advanced 802.11b coverage {data | voice} rssi-threshold *rssi*

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b parameters.
coverage	Coverage hole detection.
data	Specifies threshold for data packets.
voice	Specifies threshold for voice packets.
rssi-threshold	Receive signal strength indication threshold.
<i>rssi</i>	Valid values are from -60 to -90 dBm.

Defaults

- Data packets: -80 dBm.
- Voice packets: -75 dBm.

Usage Guidelines

The *rssi* value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data or voice queue with an RSSI value that is below the value that you enter here, a potential coverage hole has been detected.

The access point takes RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11b coverage packet-count** and **config advanced 802.11b 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 802.11b coverage level global** and **config advanced 802.11b coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

```
> config advanced 802.11b coverage data rssi-threshold -70
```

Related Commands

config advanced 802.11b coverage
config advanced 802.11b coverage exception global
config advanced 802.11b coverage fail-rate
config advanced 802.11b coverage level global
config advanced 802.11b coverage packet-count
show advanced 802.11b coverage

config advanced 802.11b edca-parameters

To enable a specific enhanced distributed channel access (EDCA) profile on the 802.11b network, use the **config advanced 802.11b edca-parameters** command.

```
config advanced 802.11b edca-parameters { wmm-default | svp-voice | optimized-voice |
optimized-video-voice }
```

Syntax	Description
config	Configure parameters.
advanced 802.11b	Advanced 802.11b parameters.
edca-parameters	Enables a specific EDCA profile.
wmm-default	Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network.
svp-voice	Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls.
optimized-voice	Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network.
optimized-video-voice	Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
Note	If you deploy video services, admission control (ACM) must be disabled.

Defaults

config advanced 802.11b edca-parameters wmm-default

Examples

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

Related Commands

show 802.11b
config advanced 802.11a edca-parameters

config advanced 802.11b factory

To reset 802.11b/g advanced settings back to the factory defaults, use the **config advanced 802.11b factory** command.

config advanced 802.11b factory

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	factory	Return all 802.11b/g advanced settings to their factory defaults.

Defaults	None.

Examples	To reset all 802.11b/g advanced settings back to the factory defaults: > config advanced 802.11b factory

Related Commands	show advanced 802.11b channel

config advanced 802.11b group-mode

To set the 802.11b/g RF group selection mode on or off, use the **config advanced 802.11b group-mode** command.

```
config advanced 802.11b group-mode {auto | off}
```

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	group-mode	Cisco radio RF grouping.
	{auto off}	- Enter auto to set the 802.11b RF group selection to automatic update mode. - Enter off to set the 802.11b RF group selection to off.

Defaults Auto.

Usage Guidelines Use to enable or disable 802.11b/g automatic RF group selection mode.

Examples To set the 802.11b/g RF group selection mode to automatic:

```
> config advanced 802.11b group-mode auto
```

To disable the 802.11b/g RF group selection mode:

```
> config advanced 802.11b group-mode off
```

Related Commands

```
show advanced 802.11b group
config advanced 802.11a group-mode
```

config advanced 802.11b logging channel

To turn the 802.11b/g channel change logging mode on or off, use the **config advanced 802.11b logging channel** command.

config advanced 802.11b logging channel {on | off}

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
logging channel	Log channel changes.
{on off}	Enable or disable 802.11b channel logging.

Defaults

Disabled.

Examples

```
> config advanced 802.11b logging channel on
```

Related Commands

show advanced 802.11b logging
config advanced 802.11a logging channel

config advanced 802.11b logging coverage

To turn the 802.11b/g coverage profile logging mode on or off, use the **config advanced 802.11b logging coverage** command.

config advanced 802.11b logging coverage {on | off}

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	logging coverage	Log coverage changes.
	{on off}	Enable or disable 802.11b coverage profile violation logging.

Defaults	Off (disabled).

Examples	> config advanced 802.11b logging coverage on

Related Commands	show advanced 802.11b logging config advanced 802.11a logging coverage

config advanced 802.11b logging foreign

To turn the 802.11b/g foreign interference profile logging mode on or off, use the **config advanced 802.11b logging foreign** command.

config advanced 802.11b logging foreign {on | off}

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
logging foreign	Log foreign changes.
{on off}	Enable or disable foreign interference profile logging mode.

Defaults

Off (disabled).

Examples

```
> config advanced 802.11b logging foreign on
```

Related Commands

show advanced 802.11b logging
config advanced 802.11a logging foreign

config advanced 802.11b logging load

To turn the 802.11b/g load profile logging mode on or off, use the **config advanced 802.11b logging load** command.

config advanced 802.11b logging load {on | off}

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	logging load	Log load changes.
	{on off}	Enable or disable 802.11b load profile violation logging.

Defaults Off (disabled).

Examples > **config advanced 802.11b logging load on**

Related Commands **show advanced 802.11b logging**
config advanced 802.11a logging load

config advanced 802.11b logging noise

To turn the 802.11b/g noise profile logging mode on or off, use the **config advanced 802.11b logging noise** command.

config advanced 802.11b logging noise {on | off}

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
logging noise	Log noise changes.
{on off}	Enable or disable 802.11b noise profile violation logging.

Defaults

Off (disabled).

Examples

```
> config advanced 802.11b logging noise on
```

Related Commands

show advanced 802.11b logging
config advanced 802.11a logging noise

config advanced 802.11b logging performance

To turn the 802.11b/g performance profile logging mode on or off, use the **config advanced 802.11b logging performance** command.

config advanced 802.11b logging performance {on | off}

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	logging performance	Log performance changes.
	{on off}	Enable or disable 802.11b performance profile violation logging.

Defaults Off (disabled).

Examples > **config advanced 802.11b logging performance on**

Related Commands **show advanced 802.11b logging**
config advanced 802.11a logging performance

config advanced 802.11b logging txpower

To turn the 802.11b/g transmit power change logging mode on or off, use the **config advanced 802.11b logging txpower** command.

```
config advanced 802.11b logging txpower {on | off}
```

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	logging txpower	Log power changes.
	{on off}	Enable or disable 802.11b transmit power change logging.

Defaults Off (disabled).

Examples > config advanced 802.11b logging txpower off

Related Commands show advanced 802.11b logging
config advanced 802.11a logging power

config advanced 802.11b monitor channel-list

To set the 802.11b/g noise/interference/rogue monitoring channel list coverage, use the **config advanced 802.11b monitor channel-list** command.

config advanced 802.11b monitor channel-list {all | country | dca}

Syntax Description	
config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
monitor channel-list	Monitor channel list.
{all country dca}	- Enter all to monitor all channels. - Enter country to monitor channels used in configured country code. - Enter dca to monitor channels used by automatic channel assignment.

Defaults The default channel list is **country**.

Examples
 > config advanced 802.11b monitor channel-list country

Related Commands
 show advanced 802.11b monitor
 config advanced 802.11a monitor coverage

config advanced 802.11b monitor coverage

To set the 802.11b/g coverage measurement interval between 60 and 3600 seconds, use the **config advanced 802.11b monitor coverage** command.

config advanced 802.11b monitor coverage *seconds*

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
monitor coverage	Monitor coverage interval.
<i>seconds</i>	Coverage measurement interval between 60 and 3600 seconds.

Defaults

180 seconds.

Examples

To set the coverage measurement interval to 60 seconds:

```
> config advanced 802.11b monitor coverage 60
```

Related Commands

show advanced 802.11b monitor

config advanced 802.11a monitor coverage

config advanced 802.11b monitor load

To set the 802.11b/g load measurement interval between 60 and 3600 seconds, use the **config advanced 802.11b monitor load** command.

config advanced 802.11b monitor load *seconds*

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	monitor load	Monitor load interval.
	<i>seconds</i>	Load measurement interval between 60 and 3600 seconds.

Defaults	60 seconds.

Examples	To set the load measurement interval to 60 seconds: > config advanced 802.11b monitor load 60

Related Commands	show advanced 802.11b monitor config advanced 802.11a monitor load

config advanced 802.11b monitor mode

To enable or disable the 802.11b monitor mode, use the **config advanced 802.11b monitor mode** command.

```
config advanced 802.11b monitor mode {enable | disable}
```

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b parameters.
	monitor mode	Monitor mode.
	{enable disable}	Enable or disable 802.11b access point monitoring.

Defaults Enabled.

Examples > config advanced 802.11b monitor mode enable

Related Commands show advanced 802.11b monitor
config advanced 802.11a monitor mode

config advanced 802.11b monitor noise

To set the 802.11b/g noise measurement interval between 60 and 3600 seconds, use the **config advanced 802.11b monitor noise** command.

config advanced 802.11b monitor noise *seconds*

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	monitor noise	Monitor noise interval.
	<i>seconds</i>	Noise measurement interval between 60 and 3600 seconds.

Defaults	180 seconds.

Examples	To set the noise measurement interval to 120 seconds: > config advanced 802.11b monitor noise 120

Related Commands	show advanced 802.11b monitor config advanced 802.11a monitor noise

config advanced 802.11b monitor signal

To set the 802.11b/g signal measurement interval between 60 and 3600 seconds, use the **config advanced 802.11b monitor signal** command.

config advanced 802.11b monitor signal *seconds*

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	monitor signal	Monitor signal interval.
	<i>seconds</i>	Signal measurement interval between 60 and 3600 seconds.

Defaults 60 seconds.

Examples To set the signal measurement interval to 120 seconds:
> **config advanced 802.11b monitor signal 120**

Related Commands **show advanced 802.11b monitor**
config advanced 802.11a monitor signal

config advanced 802.11b profile clients

To set the number of 802.11b/g Cisco lightweight access point clients threshold between 1 and 75 clients, use the **config advanced 802.11b profile clients** command.

config advanced 802.11b profile clients {**global** | *Cisco_AP*} *clients*

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	profile clients	Client profiles.
	{ global <i>Cisco_AP</i> }	Global or Cisco lightweight access point specific profile.
	<i>clients</i>	802.11b Cisco lightweight access point clients threshold between 1 and 75 clients.

Defaults 12 clients

Examples To set the Cisco lightweight access point clients threshold for all Cisco radios to 25:

```
> config advanced 802.11b profile clients global 25
```

To set the Cisco lightweight access point clients threshold for AP1 to 75:

```
> config advanced 802.11b profile clients AP1 75
```

Related Commands config advanced 802.11a profile clients

config advanced 802.11b profile customize

To turn customization on or off for an 802.11b/g Cisco lightweight access point performance profile, use the **config advanced 802.11b profile customize** command.

config advanced 802.11b profile customize *Cisco_AP* {**on** | **off**}

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	profile customize	Customize the performance profile for a Cisco lightweight access point.
	<i>Cisco_AP</i>	Cisco lightweight access point name.
	{ on off }	- Enter on to customize performance profiles for the specified Cisco lightweight access point . - Enter off to use global default performance profiles for the specified Cisco lightweight access point.

Defaults Off

Examples To turn customization on for the AP1 performance profile:

```
> config advanced 802.11b profile customize on
```

Related Commands **config advanced 802.11a profile customize**

config advanced 802.11b profile foreign

To set the foreign 802.11b/g transmitter interference threshold between 0 and 100 percent, use the **config advanced 802.11b profile foreign** command.

config advanced 802.11b profile foreign { **global** | *Cisco_AP* } *percent*

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	profile foreign	Foreign interference profile.
	{ global <i>Cisco_AP</i> }	Global or Cisco lightweight access point specific profile.
	<i>percent</i>	802.11b foreign 802.11b interference threshold between 0 and 100 percent.

Defaults 10.

Examples

To set the foreign 802.11b/g transmitter interference threshold for the whole 802.11b/g network to 50 percent:

```
> config advanced 802.11b profile foreign global 50
```

To set the foreign 802.11b/g transmitter interference threshold for AP1 to 0 percent:

```
> config advanced 802.11b profile foreign AP1 0
```

Related Commands config advanced 802.11b profile foreign

config advanced 802.11b profile noise

To set the 802.11b/g foreign noise threshold between -127 and 0 dBm, use the **config advanced 802.11b profile noise** command.

```
config advanced 802.11b profile noise {global | Cisco_AP} dBm
```

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	profile noise	Cisco lightweight access point profile noise
	{global Cisco_AP}	Global or Cisco lightweight access point specific profile
	dBm	802.11b foreign noise threshold between -127 and 0 dBm.

Defaults -70 dB

Examples

To set the 802.11b/g foreign noise threshold for the whole 802.11b/g network to -90 dBm:

```
> config advanced 802.11b profile noise global -90
```

To set the 802.11b/g foreign noise threshold for AP1 to -30 dBm:

```
> config advanced 802.11b profile noise AP1 -30
```

Related Commands config advanced 802.11a profile noise

config advanced 802.11b profile throughput

To set the 802.11b/g Cisco lightweight access point throughput threshold between 1000 and 10000000 bytes per second, use the **config advanced 802.11b profile throughput** command.

config advanced 802.11b profile throughput {*global* | *Cisco_AP*} *rate*

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	profile throughput	Throughput profile.
	{ <i>global</i> <i>Cisco_AP</i> }	Global or Cisco lightweight access point specific profile.
	<i>rate</i>	1,000 to 10,000,000 bps.

Defaults	1,000,000 bps

Examples	To set the Cisco lightweight access point throughput threshold for all Cisco radios to 1000 bytes per second: <pre>> config advanced 802.11b profile throughput global 1000</pre> To set the Cisco lightweight access point throughput threshold for AP1 to 10000000 bytes per second: <pre>> config advanced 802.11b profile throughput AP1 10000000</pre>

Related Commands	config advanced 802.11a profile throughput

config advanced 802.11b profile utilization

To set the 802.11b/g RF utilization threshold between 0 and 100 percent, use the **config advanced 802.11b profile utilization** command.

config advanced 802.11b profile utilization { **global** | *Cisco_AP* } *percent*

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
profile utilization	Cisco lightweight access point profile utilization
{ global <i>Cisco_AP</i> }	Global or Cisco lightweight access point specific profile
<i>percent</i>	802.11b RF utilization threshold between 0 and 100 percent.

Defaults

80%

Examples

To set the RF utilization threshold for the whole 802.11b/g network to 100 percent:

```
> config advanced 802.11b profile utilization global 100
```

To set the RF utilization threshold for the AP1 to 50 percent:

```
> config advanced 802.11b profile utilization AP1 50
```

Related Commands

config advanced 802.11a profile utilization

config advanced 802.11b receiver

To set the advanced receiver configuration, use the **config advanced 802.11b receiver** command.

config advanced 802.11b receiver {default | rxstart}

Syntax Description	
config	Configure parameters.
advanced 802.11b	Advanced 802.11b parameters.
receiver	Receiver configuration.
{default rxstart}	- Enter default to specify default advanced receiver configuration. - Enter rxstart to specify advanced receiver start configuration.

Defaults None.

Examples Cannot change receiver params while network is enabled:
 > **config advanced 802.11b receiver default**

Related Commands config advanced 802.11a receiver

config advanced 802.11b receiver pico-cell-V2

If pico cell mode version 2 is enabled, use the **config advanced 802.11b receiver pico-cell-V2** command to configure the receive sensitivity.

```
config advanced 802.11b receiver pico-cell-V2 {rx_sense_threshold | cca_sense_threshold |
sta_tx_pwr} min max current
```

Syntax Description		
config		Configure parameters.
advanced 802.11b		Advanced 802.11b parameters.
receiver		Receiver configuration.
pico-cell-V2		Pico cell version 2 parameters
rx_sense_threshold		Configure the receive sensitivity threshold
cca_sense_threshold		Configure the CCA sensitivity threshold
sta_tx_pwr		To configure the transmit power
<i>min max current</i>		Measured in dBm.

Defaults None.

Examples

```
> config advanced 802.11b receiver pico-cell-V2 rx_sense_threshold -127 127 10
> config advanced 802.11b receiver pico-cell-V2 cca_sense_threshold -127 127 10
> config advanced 802.11b receiver pico-cell-V2 sta_tx_power -127 127 -65
```

Related Commands

```
config advanced 802.11a receiver
config advanced 802.11b receiver pico-cell-V2 send_iapp_req client_mac
```


config advanced 802.11b receiver pico-cell-V2 send_iapp_req

If pico cell mode version 2 is enabled and you want to transmit a unicast IAPP high-density frame request to a specific client, enter this command:

config advanced 802.11b receiver pico-cell-V2 send_iapp_req *client_mac*

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b parameters.
receiver	Receiver configuration.
pico-cell-V2	Pico cell version 2 parameters
send_iapp_req	Send a unicast IAPP high-density frame request
<i>client_mac</i>	Specify the client mac address

Defaults

None.

Examples

```
> config advanced 802.11b receiver pico-cell-V2 send_iapp_req 10:2b:3c:4d:5e:62
```

Related Commands

config advanced 802.11a receiver

config advanced 802.11b receiver pico-cell-V2 {rx_sense_threshold | cca_sense_threshold | sta_tx_pwr} *min max current*

config advanced 802.11b txpower-update

To initiate updates of the 802.11b transmit power for every Cisco lightweight access point, use the **config advanced 802.11b txpower-update** command.

config advanced 802.11b txpower-update

Syntax Description	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b parameters.
	txpower-update	Update transmission power

Defaults None.

Examples > **config advanced 802.11b txpower-update**

Related Commands **config advance 802.11a txpower-update**

config advanced arp

To configure advanced address resolution protocol (ARP) settings, use the **config advanced arp** command.

show advanced arp [padding *number*]

Syntax	Description
padding	Configures the amount of padding to be added to an ARP frame.
<i>number</i>	Specifies the number (0 to 32 bytes) of padding characters.

Defaults
None.

Examples
> config advanced arp padding 5

Related Commands
show advanced arp

config advanced backup-controller primary

To configure a primary backup controller for a specific controller, use the **config advanced backup-controller primary** command.

```
config advanced backup-controller primary backup_controller_name
backup_controller_ip_address
```

Syntax Description	config	Configure parameters.
	advanced	Advanced parameters.
	backup-controller primary	Configure the primary backup controller.
	backup_controller_name	Name of the backup controller.
	backup_controller_ip_address	IP address of the backup controller.

Defaults None.

Usage Guidelines To delete a primary backup controller entry, enter 0.0.0.0 for the controller IP address.

Examples > config advanced backup-controller primary Controller_1 10.10.10.10

Related Commands show advanced backup-controller

config advanced backup-controller secondary

To configure a primary backup controller for a specific controller, use the **config advanced backup-controller secondary** command.

```
config advanced backup-controller secondary backup_controller_name
backup_controller_ip_address
```

Syntax Description	config	Configure parameters.
	advanced	Advanced parameters.
	backup-controller secondary	Configure the secondary backup controller.
	backup_controller_name	Name of the backup controller.
	backup_controller_ip_address	IP address of the backup controller.

Defaults None.

Usage Guidelines To delete a secondary backup controller entry, enter 0.0.0.0 for the controller IP address.

Examples > config advanced backup-controller secondary Controller_1 10.10.10.10

Related Commands show advanced backup-controller

config advanced client-handoff

To set the client handoff to occur after a selected number of 802.11 data packet excessive retries, use the **config advanced client-handoff** command.

config advanced client-handoff *num_of_retries*

Syntax Description

config	Configure parameters.
advanced	Advanced parameters.
client-handoff	Client handoff.
<i>num_of_retries</i>	Number of excessive retries before client handoff (from 0 to 255).

Defaults

0 excessive retries (disabled).

Examples

To set the client handoff to 100 excessive retries:

```
> config advanced client-handoff 100
```

Related Commands

show advanced client-handoff

config advanced eap

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

```
config advanced eap [ eapol-key-timeout timeout | eapol-key-retries retries |
  identity-request-timeout timeout |
  identity-request-retries retries |
  key-index index |
  max-login-ignore-identity-response {enable | disable}
  request-timeout timeout |
  request-retries retries ]
```

Syntax Description		
eapol-key-timeout	(Optional)	Specifies the amount of time (1 to 5 seconds) in which the controller attempts to send an EAP key over the LAN to wireless clients using local EAP.
eapol-key-retries	(Optional)	Specifies the maximum number of times (0 to 4 retries) that the controller attempts to send an EAP key over the LAN to wireless clients using local EAP.
identity-request-timeout	(Optional)	Specifies the amount of time (1 to 120 seconds) in which the controller attempts to send an EAP identity request to wireless clients using local EAP.
identity-request-retries	(Optional)	Specifies the maximum number of times (1 to 20 retries) that the controller attempts to retransmit the EAP identity request to wireless clients using local EAP.
key-index	(Optional)	index—Specifies the key index (0 or 3) used for dynamic wired equivalent privacy (WEP).
max-login-ignore-identity-response	(Optional)	Specifies that the maximum EAP identity response login count for a user is ignored. When enabled, this command limits the number of devices that can be connected to the controller with the same username.
request-timeout	(Optional)	Specifies the amount of time (1 to 120 seconds) in which the controller attempts to send an EAP request to wireless clients using local EAP..
request-retries	(Optional)	Specifies the maximum number of times (1 to 120 retries) that the controller attempts to retransmit the EAP request to wireless clients using local EAP.

Defaults

Default for **eapol-key-timeout**: 1 second.

Default for **eapol-key-retries**: 2 retries.

Examples

```
> config advanced eap key-index 0
```

Related Commands

show advanced eap

config advanced rate

To enable or disable switch control path rate limiting, use the **config advanced rate** command.

config advanced rate [**enable** | **disable**]

Syntax Description

enable	Enables the feature.
disable	Disables the feature.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> config ap tftp-downgrade 10.0.23.8 1238.tar ap1240_102301
```

Related Commands

None.

config advanced statistics

To enable or disable Cisco Wireless LAN controller port statistics collection, use the **config advanced statistics** command.

config advanced statistics {enable | disable}

Syntax Description

config	Configure parameters.
advanced	Advanced parameters.
statistics	Statistics.
{enable disable}	Enable or disable switch port statistics.

Defaults

Enabled.

Examples

To disable statistics:

```
> config advanced statistics disable
```

Related Commands

show advanced statistics
show stats port
show stats switch

Configure Advanced Timers Commands

User the **advanced timers** commands to configure advanced 802.11a settings.

config advanced timers ap-discovery-timeout

The Cisco lightweight access point discovery time-out is how often a Cisco Wireless LAN controller attempts to discover unconnected Cisco lightweight access points. To configure the Cisco lightweight access point discovery time-out, use the **config advanced timers ap-discovery-timeout** command.

config advanced timers ap-discovery-timeout *seconds*

Syntax Description	config	Configure parameters.
	advanced	Advanced parameters.
	timers	Network timers.
	ap-discovery-timeout	Cisco lightweight access point discovery timeout.
	<i>seconds</i>	Timeout value between 1 and 10 seconds.

Defaults 10 seconds.

Examples > **config advanced timers ap-discovery-timeout 20**

Related Commands

- [show advanced timers](#)
- [config advanced timers ap-fast-heartbeat](#)
- [config advanced timers ap-heartbeat-timeout](#)
- [config advanced timers ap-primary-discovery-timeout](#)
- [config advanced timers auth-timeout](#)

config advanced timers ap-fast-heartbeat

To enable or disable the fast heartbeat timer thus reducing the amount of time it takes to detect a controller failure for local, hybrid-REAP, or all access points, use the **config advanced timers ap-fast-heartbeat** command.

config advanced timers ap-fast-heartbeat {local | hreap | all} {enable | disable} *interval*

Syntax Description	
config	Configure parameters.
advanced	Advanced parameters.
timers	Network timers.
ap-fast-heartbeat	Configure the fast heartbeat interval
{local hreap all}	- Enable local to configure the fast heartbeat interval for access points in local mode only. - Enable hreap to configure the fast heartbeat interval for access points in hybrid-REAP mode only. - Enable all to configure the fast heartbeat interval for all access points.
{enable disable}	- Select enable to enable a fast heartbeat interval. - Select disable to disable a fast heartbeat interval
<i>interval</i>	Specify a small heartbeat interval (between 1 and 10 seconds inclusive) reduces the amount of time it takes to detect a controller failure.

Defaults Disabled.

Examples

```
> config advanced timers ap-fast-heartbeat local enable 5
> config advanced timers ap-fast-heartbeat hreap enable 8
> config advanced timers ap-fast-heartbeat all enable 6
> config advanced timers ap-fast-heartbeat all disable
```

Related Commands

[show advanced timers](#)
[config advanced timers ap-discovery-timeout](#)
[config advanced timers ap-heartbeat-timeout](#)
[config advanced timers ap-primary-discovery-timeout](#)
[config advanced timers auth-timeout](#)

config advanced timers ap-heartbeat-timeout

The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keep-alive signal to the Cisco Wireless LAN controller. To configure the Cisco lightweight access point heartbeat timeout, use the **config advanced timers ap-heartbeat-timeout** command.

config advanced timers ap-heartbeat-timeout *seconds*

Syntax Description	config	Configure parameters.
	advanced	Advanced parameters.
	timers	Network timers.
	ap-heartbeat-timeout	Cisco lightweight access point heartbeat timeout.
	<i>seconds</i>	Timeout value between 1 and 30 seconds.

Defaults	30 seconds.

Usage Guidelines	This <i>seconds</i> value should be at least three times larger than the fast heartbeat timer.

Examples	> config advanced timers ap-heartbeat-timeout 20

Related Commands	show advanced timers config advanced timers ap-discovery-timeout config advanced timers ap-fast-heartbeat config advanced timers ap-primary-discovery-timeout config advanced timers auth-timeout

config advanced timers ap-primary-discovery-timeout

To configure the access point primary discovery request timer, use the **config advanced timers ap-primary-discovery-timeout** command.

config advanced timers ap-primary-discovery-timeout *interval*

Syntax Description	config	Configure parameters.
	advanced	Advanced parameters.
	timers	Network timers.
	ap-primary-discovery-timeout	Configure the amount of time the access point will wait for a discovery response from a controller.
	<i>interval</i>	Timeout value between 30 and 3600 seconds.

Defaults 120 seconds.

Examples > **config advanced timers ap-primary-discovery-timeout 1200**

Related Commands

- [show advanced timers](#)
- [config advanced timers ap-discovery-timeout](#)
- [config advanced timers ap-fast-heartbeat](#)
- [config advanced timers ap-heartbeat-timeout](#)
- [config advanced timers auth-timeout](#)

config advanced timers auth-timeout

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

config advanced timers auth-timeout *seconds*

Syntax Description	config	Configure parameters.
	advanced	Advanced parameters.
	timers	Network timers.
	auth-timeout	Authentication response timeout.
	<i>seconds</i>	Timeout value in seconds between 10 and 600.

Defaults	10 seconds.

Examples	> config advanced timers auth-timeout 20

Related Commands	show advanced timers config advanced timers ap-fast-heartbeat config advanced timers ap-discovery-timeout config advanced timers ap-heartbeat-timeout config advanced timers ap-primary-discovery-timeout

config advanced timers eap-timeout

To configure the EAP expiration timeout, use the **config advanced timers eap-timeout** command.

config advanced timers eap-timeout *seconds*

Syntax Description	config	Configure parameters.
	advanced	Advanced parameters.
	timers	Network timers.
	eap-timeout	EAP timeout.
	<i>seconds</i>	Timeout value in seconds between 8 and 120.

Defaults	None.

Examples	> config advanced timers eap-timeout 10

Related Commands	show advanced timers

config advanced timers eap-identity-request-delay

To configure the advanced EAP identity request delay in seconds, use the **config advanced timers eap-identity-request-delay** command.

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

Syntax Description	show	Displays configurations.
	advanced	Advanced parameters.
	timers	Advanced system timers.
	eap-identity-request-delay	
	<i>seconds</i>	Number of seconds between 0 and 10.

Defaults None.

Examples > **show advanced timers eap-identity-request-delay 8**

Related Commands config advanced timers auth-timeout, config advanced timers rogue-ap, show advanced timers

Configure Access Point Commands

User the **config ap** commands to configure access point settings.

config ap add

To add a Foreign Access Point, use the **config ap add** command.

config ap add *MAC port {enable | disable} IP_address*

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	add	Add a Foreign Access Point.
	<i>MAC</i>	Foreign Access Point MAC address.
	<i>port</i>	Port number for accessing the Foreign Access Point.
	{enable disable}	Enable or disable 802.1X authentication for a Foreign Access Point.
	<i>IP_address</i>	IP Address for a Foreign Access Point. A value of 0 (default) means that the address is assigned by a DHCP server.

Defaults	None.

Examples	> config ap add 12:12:12:12:12:12 2033 enable 192.12.12.1

Related Commands	config ap

config ap bhmode

To configure the Cisco Bridge Backhaul Mode, use the **config ap bhmode** command.

```
config ap bhmode {11a | 11b | 11g} Cisco_AP
```

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	bhmode	Configure the Cisco Bridge Backhaul Mode.
	{11a 11b 11g}	- Enter 11a to set 11a as the Cisco Bridge Backhaul Mode. - Enter 11b to set 11b as the Cisco Bridge Backhaul Mode. - Enter 11g to set 11g as the Cisco Bridge Backhaul Mode.
	Cisco_AP	Name of a Cisco lightweight access point.

Defaults None.

Examples

```
> config ap bhmode 11g AP02
```

Changing the AP's backhaul mode will cause the AP to reboot.
Are you sure you want to continue? (y/n)

Related Commands config ap

config ap bhrate

To configure the Cisco Bridge Backhaul Tx Rate, use the **config ap bhrate** command.

config ap bhrate *rate Cisco_AP*

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	bhrate	Configure Cisco Bridge Backhaul Tx Rate.
	<i>rate</i>	Cisco Bridge Backhaul Tx Rate in Kbps. The legal values are: 6000, 12000, 18000, 24000, 36000, 48000, and 54000.
	<i>Cisco_AP</i>	Name of a Cisco lightweight access point.

Defaults	None.

Examples	> config ap bhrate 54000 AP01

Related Commands	config ap

config ap bridgegroupname

To set or delete bridgegroupname on a Cisco lightweight access point, use the **config ap bridgegroupname** command.



Note

Only access points with the same bridgegroupname can connect to each other.

config ap bridgegroupname {set *groupname* | delete} *Cisco_AP*

Syntax Description

config	Displays configurations.
ap	Advanced parameters.
bridgegroupname	Set or delete bridgegroupname on a Cisco lightweight access point.
{set <i>groupname</i> delete}	- Enter set <i>groupname</i> to set a Cisco lightweight access point's bridgegroupname. - Enter delete to delete a Cisco lightweight access point's bridgegroupname.
<i>Cisco_AP</i>	Name of a Cisco lightweight access point.

Defaults

None.

Examples

> **config ap bridgegroupname delete AP02**

Changing the AP's bridgegroupname may strand the bridge AP. Please continue with caution.
Changing the AP's bridgegroupname will also cause the AP to reboot.
Are you sure you want to continue? (y/n)

Related Commands

config ap

config ap bridging

To enable or disable Ethernet-to-Ethernet bridging on a Cisco lightweight access point, use the **config ap bridging** command.

config ap bridging {enable | disable} *Cisco_AP*

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	bridging	enable or disable Ethernet-to-Ethernet bridging on a Cisco lightweight access point.
	{enable disable}	Enable or disable Ethernet-to-Ethernet bridging.
	<i>Cisco_AP</i>	Name of a Cisco lightweight access point.

Defaults None.

Examples

To enable bridging on an access point enter:

```
config ap bridging enable nyc04-44-1240
```

To disable bridging on an access point enter:

```
config ap bridging disable nyc04-44-1240
```

Related Commands **config ap**

config ap cdp

To enable or disable Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **config ap cdp** command.

config ap cdp {enable | disable} {Cisco_AP | all}

Syntax Description

config	Configure parameters.
ap	Configure lightweight access points.
cdp	Cisco Discovery Protocol.
enable disable	Enable or disable CDP.
<i>Cisco_AP</i> all	Name of a Cisco lightweight access point or all to specify all access points.

Defaults

Disabled.

Usage Guidelines

The **config ap cdp disable all** command disables CDP on all access points that are joined to the controller and all access points that join in the future. CDP remains disabled on both current and future access points even after the controller or access point reboots. To enable CDP, enter **config ap cdp enable all**.



Note

After you enable CDP on all access points joined to the controller, you may disable and then re-enable CDP on individual access points using **config ap cdp {enable | disable} Cisco_AP**. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.

Examples

```
> config ap cdp enable all
> config ap cdp disable ap02
```

Related Commands

config cdp {enable | disable}
config cdp advertise
config cdp holdtime
config cdp timer
debug cdp events
debug cdp packets
show ap cdp neighbors detail
show cdp entry all
show cdp traffic

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 {enable IP_address filename {compress | uncompress} | disable}
                        {Cisco_AP | all}
```

Syntax Description	
config	Displays configurations.
ap	Advanced parameters.
core-dump	Configure a Cisco lightweight access point's memory core dump.
{enable disable}	Enable or disable Ethernet-to-Ethernet bridging.
<i>IP_address</i>	IP Address for the TFTP server.
<i>filename</i>	Image file name on the TFTP server.
{compress uncompress}	- Enter compress to compress the core dump file. - Enter uncompress to not compress the core dump file.
{Cisco_AP all}	Name of a Cisco lightweight access point or all to specify all access points.

Defaults None.

Examples > **config ap core-dump enable 192.1.1.1 log compress AP02**

Related Commands **config ap**

config ap crash-file clear-all

To delete all crash and radio core dump files, use the **config ap crash-file clear-all** command.

config ap crash-file clear-all

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	crash-file clear-all	Delete all crash and radio core dump files.

Defaults	None.

Examples	> <code>config ap crash-file clear-all</code>

Related Commands	<code>config ap</code>

config ap crash-file delete

To delete a single crash or radio core dump file, use the **config ap crash-file delete** command.

config ap crash-file delete *filename*

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	crash-file delete	Delete a single crash or radio core dump file.
	<i>filename</i>	Name of the file to delete.

Defaults	None.

Examples	> config ap crash-file delete crash-file-1

Related Commands	config ap

config ap crash-file get-crash-file

To collect the latest crash data for a Cisco lightweight access point, use the **config ap crash-file get-crash-file** command. Use the [transfer upload datatype](#) command to transfer the collected data to the Cisco Wireless LAN controller.

```
config ap crash-file get-crash-file Cisco_AP
```

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	crash-file	Collect the latest crash data for an access point.
	get-crash-file	
	Cisco_AP	Name of the Cisco lightweight access point.

Defaults None.

Examples > config ap crash-file get-crash-file AP3

Related Commands config ap crash-file delete

config ap crash-file get-radio-core-dump

To get a Cisco lightweight access point’s radio core dump, use the **config ap crash-file get-radio-core-dump** command.

config ap crash-file get-radio-core-dump *Slot_ID* *Cisco_AP*

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	crash-file radio-core-dump	Get a Cisco lightweight access point’s radio core dump.
	<i>Slot_ID</i>	The slot ID (either 0 or 1).
	<i>Cisco_AP</i>	Name of a Cisco lightweight access point.

Defaults	None.

Examples	> config ap crash-file get-radio-core-dump 0 AP02

Related Commands	config ap

config ap delete

To delete a Foreign Access Point, use the **config ap delete** command.

config ap delete *MAC*

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	delete	Delete a Foreign Access Point.
	<i>MAC</i>	Foreign Access Point MAC address.

Defaults	None.

Examples	> config ap delete 12:12:12:12:12:12

Related Commands	config ap

config ap dot1xuser

To configure the global authentication username and password for all access points currently joined to the controller as well as any access points that join the controller in the future, enter this command. Alternatively, you can set the values for a specific access point.

config ap dot1xuser add username *user* **password** *password* {**all** | *Cisco_AP*}

Syntax Description		
config		Configure parameters.
ap		Cisco lightweight access point.
dot1xuser		Descriptive location.
add username		Add username.
<i>user</i>		Specify username.
password		Add password.
<i>password</i>		Specify password.
all		For all access points.
<i>Cisco_AP</i>		For a specific access point.

Defaults None.

Usage Guidelines You must enter a strong *password*. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of upper- and lowercase letters, numbers, and symbols.
- They are not a word in any language.

Examples

```
config ap dot1xuser add username cisco123 password cisco2020 all
config ap dot1xuser add username cisco123 password cisco2020 Cisco_AP
```

Related Commands

- [config ap dot1xuser delete](#)
- [config ap dot1xuser disable](#)
- [show ap summary](#)

config ap dot1xuser delete

To force a specific access point to use the controller’s global authentication settings, enter the following command:

```
config ap dot1xuser delete Cisco_AP
```

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	dot1xuser	Descriptive location.
	delete	Delete authentication.
	Cisco_AP	Specify the access point.

Defaults

None.

Examples

config ap mgmtuser delete Cisco_AP1

Related Commands

config ap dot1xuser

config ap dot1xuser disable

show ap summary

config ap dot1xuser disable

To disable authentication for all access points or for a specific access point, enter the following command:

```
config ap dot1xuser disable {all | Cisco_AP}
```

Syntax Description

config	Configure parameters.
ap	Cisco lightweight access point.
dot1xuser	Descriptive location.
disable	Delete authentication.
all	For all access points.
<i>Cisco_AP</i>	Specify the access point

Defaults

None.

Usage Guidelines

You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

Examples

```
config ap mgmtuser disable Cisco_AP1
```

Related Commands

[config ap dot1xuser](#)
[config ap dot1xuser delete](#)
[show ap summary](#)

config ap disable

To disable a Cisco lightweight access point, use the **config ap disable** command.

config ap disable *Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Cisco lightweight access point.
disable	Disable command.
<i>Cisco_AP</i>	Name of the Cisco lightweight access point.

Defaults

None.

Examples

```
> config ap disable AP1
```

Related Commands

config ap enable

config ap enable

To enable a Cisco lightweight access point, use the **config ap enable** command.

config ap enable *Cisco_AP*

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	enable	Enable command.
	<i>Cisco_AP</i>	Name of the Cisco lightweight access point.

Defaults	None.

Examples	> config ap enable AP1

Related Commands	config ap disable

config ap group-name

To specify a descriptive group name for a Cisco lightweight access point, use the **config ap group-name** command. The Cisco lightweight access point must be disabled before changing this parameter.

```
config ap group-name groupname Cisco_AP
```

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	groupname	Descriptive group name.
	Cisco_AP	Name of the Cisco lightweight access point.

Defaults	None.

Examples	> config ap group-name superusers AP01

Related Commands	show ap summary

config ap h-reap radius auth set

To configure a primary or secondary RADIUS server for a specific hybrid-REAP access point, use the **config ap h-reap radius auth set** command.

```
config ap h-reap radius auth set {primary | secondary}ip_address auth_port secret
```

Syntax Description	config ap	Configure access point.
	h-reap	Enter h-reap to specify the hybrid remote edge access point mode.
	radius auth set	
	primary	
	secondary	
	ip_address	Name of the Cisco lightweight access point.
	auth_port secret	

Defaults	None.

Examples	> config ap h-reap radius auth set primary 192.12.12.1

Related Commands	config ap mode h-reap config ap h-reap vlan wlan config ap h-reap vlan config ap h-reap vlan native

config ap h-reap vlan

To enable or disable VLAN tagging for a hybrid-REAP access, use the **config ap h-reap vlan** command.

```
config ap h-reap vlan {enable | disable} Cisco_AP
```

Syntax Description	config ap	Configure access point.
	h-reap	Enter h-reap to specify the hybrid remote edge access point mode.
	{enable disable}	Enable or disable the access point's VLAN tagging.
	<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

> config ap h-reap vlan wlan enable AP02

Related Commands

config ap mode h-reap
config ap h-reap radius auth set
config ap h-reap vlan wlan
config ap h-reap vlan native

config ap h-reap vlan native

To configure a native VLAN for a hybrid-REAP access, use the **config ap h-reap vlan native** command.

config ap h-reap vlan native *vlan-id* *Cisco_AP*

Syntax Description	config ap	Configure access point.
	h-reap	Enter h-reap to specify the hybrid remote edge access point mode.
	vlan native	The “managing” VLAN.
	<i>vlan-id</i>	VLAN identifier.
	<i>Cisco_AP</i>	Name of the Cisco lightweight access point.

Defaults None.

Examples > **config ap h-reap vlan native 6 AP02**

Related Commands

- config ap mode h-reap**
- config ap h-reap radius auth set**
- config ap h-reap vlan wlan**

config ap h-reap vlan wlan

To assign a VLAN ID to a hybrid-REAP access point, use the **config ap h-reap vlan wlan** command.

```
config ap h-reap vlan wlan ip_address vlan-id Cisco_AP
```

Syntax Description	config ap	Configure access point.
	h-reap	Enter h-reap to specify the hybrid remote edge access point mode.
	ip_address	Name of the Cisco lightweight access point.
	vlan-id	VLAN identifier.
	Cisco_AP	Name of the Cisco lightweight access point.

Defaults	VLAN ID associated to the WLAN.

Examples	> config ap h-reap vlan wlan 192.12.12.1 6 AP02

Related Commands	config ap mode h-reap config ap h-reap radius auth set config ap h-reap vlan config ap h-reap vlan native

config ap led-state

To enable or disable the LED-State for an access point, use the **config ap led-state** command.

```
config ap led-state {enable | disable} {Cisco_AP | all}
```

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	led-state	Enable or disable the LED-State for an access point.
	{enable disable}	Enable or disable the access point's LED-State.
	{Cisco_AP all}	Name of a Cisco lightweight access point or all to specify all access points.

Defaults	None.

Examples	> config ap led-state enable AP02

Related Commands	config ap

config ap link-latency

To enable or disable link latency for a specific access point or for all access points currently associated to the controller, enter this command:

```
config ap link-latency {enable | disable | reset} {Cisco_AP | all}
```

Syntax Description

config	Configure parameters.
ap	Cisco lightweight access point.
link-latency	Configure link-latency.
enable disable	Enable or disable link-latency.
reset	Reset all link-latency statistics.
<i>Cisco_AP</i>	Name of the Cisco lightweight access point.
all	Configure all Cisco access points.

Defaults

Link latency is disabled by default.

Usage Guidelines

This command enables or disables link latency only for access points that are currently joined to the controller. It does not apply to access points that join in the future.

Examples

```
>config ap link-latency enable all
```

Related Commands

[show ap config](#)

config ap location

To modify the descriptive location of a Cisco lightweight access point, use the **config ap location** command. The Cisco lightweight access point must be disabled before changing this parameter.

config ap location *location* *Cisco_AP*

Syntax	Description
config	Configure parameters.
ap	Cisco lightweight access point.
location	Descriptive location.
<i>location</i>	Location name (enclosed by double quotation marks).
<i>Cisco_AP</i>	Name of the Cisco lightweight access point.

Defaults	None.

Examples	> config ap location "Building 1" AP1

Related Commands	show ap summary

config ap mgmtuser

To configure the global username, password, and enable password for all access points currently joined to the controller as well as any access points that join the controller in the future, enter this command. Alternatively, you can set the values for a specific access point.

```
config ap mgmtuser add username user password password enablesecret enable_password {all
| Cisco_AP}
```

Syntax Description

config	Configure parameters.
ap	Cisco lightweight access point.
mgmtuser	Descriptive location.
add username	Add username.
<i>user</i>	Specify username.
password	Add password.
<i>password</i>	Specify password.
enablesecret	Add configuration password.
<i>enable_password</i>	Specify password.
all	For all access points.
<i>Cisco_AP</i>	For a specific access point.

Defaults

None.

Examples

```
> config ap mgmtuser add username cisco123 password cisco2020 enablesecret cisco0202 all
> config ap mgmtuser add username cisco123 password cisco2020 enablesecret cisco0202
Cisco_AP
```

Related Commands

show ap summary
config ap mgmtuser delete

config ap mgmtuser delete

To force a specific access point to use the controller's global credentials, enter the following command:

```
config ap mgmtuser delete Cisco_AP
```

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	mgmtuser	Descriptive location.
	delete	Delete local credentials.
	<i>Cisco_AP</i>	Specify the access point

Defaults	None.

Examples	<pre>>config ap mgmtuser delete Cisco_AP1</pre>

Related Commands	<code>show ap summary</code>

config ap mode

Cisco wireless LAN controllers communicate with Cisco lightweight access points in a variety of modes. 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 {local | reap | monitor | rogue | sniffer | bridge} Cisco_AP
```

Syntax Description	config ap mode	Configure boot option.
	{local reap monitor rogue sniffer bridge}	You have six choices: • Enter local to specify the local mode. • Enter reap to specify the remote edge access point mode. • Enter monitor to specify the monitor-only mode. • Enter rogue to specify the rogue detector mode. • Enter sniffer to specify the wireless sniffer mode. • Enter bridge to specify the bridge access point mode.
	Cisco_AP	Name of the Cisco lightweight access point.

Defaults Local.

Examples

Sets the Cisco Wireless LAN controller to communicate with AP01 in local (normal) mode:

```
> config ap mode local AP01
```

Sets the Cisco Wireless LAN controller to communicate with Cisco lightweight access point AP91 in remote office mode:

```
> config ap mode reap AP91
```

Sets the Cisco Wireless LAN controller to communicate with AP02 in monitor (listen-only) mode:

```
> config ap mode monitor AP02
```

Sets the AP91 in rogue access point detector mode:

```
> config ap mode rogue AP91
```

Sets the AP02 in wireless sniffer mode. It will capture and forward all the packets from the clients on that channel to a remote machine that runs AiroPeek (A packet analyzer for IEEE 802.11 wireless LANs). It will include information on timestamp, signal strength, packet size and so on.

```
> config ap mode sniffer AP02
```

Sets the AP91 in bridge mode:

```
> config ap mode bridge AP91
```

Related Commands show ap config

config ap mode h-reap

To enable hybrid REAP for an access point, use the **config ap mode h-reap** command.

config ap mode h-reap *Cisco_AP*

Syntax Description	config ap mode	Configure boot option.
	h-reap	Enter h-reap to specify the hybrid remote edge access point mode.
	<i>Cisco_AP</i>	Name of the Cisco lightweight access point.

Defaults	None.

Examples	> config ap mode h-reap AP01

Related Commands	config ap h-reap radius auth set config ap h-reap vlan wlan config ap h-reap vlan config ap h-reap vlan native

config ap name

To modify the name of a Cisco lightweight access point, use the **config ap name** command.

```
config ap name new_name old_name
```

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	name	Name of the Cisco lightweight access point.
	new_name	Desired Cisco lightweight access point name.
	old_name	Current Cisco lightweight access point name.

Defaults	None.

Examples	> config ap name AP1 AP2

Related Commands	show ap config

config ap port

To configure the port for a Foreign Access Point., use the **config ap port** command.

config ap port *MAC port*

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	port	Configure the port for a Foreign Access Point
	<i>MAC</i>	Foreign Access Point MAC address.
	<i>port</i>	Port number for accessing the Foreign Access Point.

Defaults	None.

Examples	> config ap port 12:12:12:12:12:12 20

Related Commands	config ap

config ap power injector

To configure the Power Injector State for an access point, use the **config ap power injector** command.

```
config ap power injector {enable | disable} {Cisco_AP | all} {installed | override | switch_MAC}
```

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	power	Configure the power injector state for an access point.
	{enable disable}	Enable or disable the power injector state for an access point.
	Cisco_AP	Name of the Cisco lightweight access point.
	all	Configure all Cisco lightweight access points connected to the controller.
	installed	Detect the MAC address of the current switch port that has a power injector.
	override	Override the safety checks and assume a power injector is always installed.
	switch_MAC	The MAC address of the switch port with an installed power injector.

Defaults None.

Examples > config ap power injector enable all 12:12:12:12:12:12

Related Commands config ap

config ap power pre-standard

To enable or disable the Inline Power Cisco Pre-Standard switch state for an access point, use the **config ap power pre-standard** command.

```
config ap power pre-standard {enable | disable} Cisco_AP
```

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	power pre-standard	Configure the Inline Power Cisco Pre-Standard switch state for an access point.
	{enable disable}	Enable or disable the Inline Power Cisco pre-standard switch state for an access point.
	Cisco_AP	Name of the Cisco lightweight access point.

Defaults	None.

Examples	> config ap power pre-standard enable AP02

Related Commands	config ap

config ap primary-base

To set the Cisco lightweight access point primary Cisco Wireless LAN controller, use the **config ap primary-base** command. The Cisco lightweight access point associates with this Cisco Wireless LAN controller for all network operation and in the event of a hardware reset.

config ap primary-base *controller_name* *Cisco_AP* [*controller_ip_address*]

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	primary-base	Cisco lightweight access point primary Cisco Wireless LAN controller.
	<i>controller_name</i>	Name of Cisco Wireless LAN controller.
	<i>Cisco_AP</i>	Cisco lightweight access point name.
	<i>controller_ip_address</i>	[Optional] If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller.

Defaults	None.

Examples	> config ap primary-base SW_1 AP2

Related Commands	show sysinfo config sysname config ap secondary-base config ap tertiary-base

config ap priority

To assign a priority designation to an access point that allows it to reauthenticate after a controller failure by priority rather than on a first-come-until-full basis, use the **config ap priority** command.

In a failover situation, if the backup controller does not have enough ports to allow all the access points in the affected area to reauthenticate, it gives priority to higher-priority access points over lower-priority ones, even if it means replacing lower-priority access points.

config ap priority {1 | 2 | 3 | 4} *Cisco_AP*

Syntax Description		
config		Configure parameters.
ap		Cisco lightweight access point.
priority		Configure AP failover priority command
{1 2 3 4}		Assign a reauthentication priority: • 1 to specify low priority • 2 to specify medium priority • 3 to specify high priority • 4 to specify highest (critical) priority
<i>Cisco_AP</i>		Cisco lightweight access point name.

Defaults

1 - Low priority.

Examples

```
> config ap priority 3 AP02
```

Related Commands

[config network ap-priority](#)
[show ap summary](#)
[show network summary](#)

config ap reporting-period

To reset a Cisco lightweight access point, use the **config ap reset** command.

config ap reporting-period *period*

Syntax Description

config	Configure parameters.
ap	Cisco lightweight access point.
reporting-period	Reporting-period command.
<i>period</i>	Time period in seconds between 10 and 120.

Defaults

None.

Examples

```
> config ap reporting-period 120
```

Related Commands

show ap config 802.11a
show ap config 802.11ab

config ap reset

To reset a Cisco lightweight access point, use the **config ap reset** command.

config ap reset *Cisco_AP*

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	reset	Reset command.
	<i>Cisco_AP</i>	Cisco lightweight access point name.

Defaults	None.

Examples	> config ap reset AP2

Related Commands	show ap config

config ap role

To configure a Cisco Bridge role of operation, use the **config ap role** command.

```
config ap role {rooftop | poletop | auto} Cisco_AP
```

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	role	Configure a Cisco Bridge role of operation.
	{ rooftop poletop auto }	Set the Cisco Bridge role of operation to rooftop , poletop , or auto . • Rooftop role for the Cisco Bridge. • Poletop role for the Cisco Bridge. • Auto Role for the Cisco Bridge.
	Cisco_AP	Name of the Cisco lightweight access point.

Defaults None.

Examples

```
> config ap role auto AP02
```

Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)

Related Commands config ap

config ap rst-button

To configure the Reset button for an access point, use the **config ap rst-button** command.

config ap rst-button {enable | disable} *Cisco_AP*

Syntax Description	config	Displays configurations.
	ap	Advanced parameters.
	rst-button	Configure the Reset button for an access point.
	{enable disable}	Enable or disable the Reset button for an access point.
	<i>Cisco_AP</i>	Name of the Cisco lightweight access point.

Defaults	None.

Examples	> config ap rst-button enable AP03

Related Commands	config ap

config ap secondary-base

To set the Cisco lightweight access point secondary Cisco Wireless LAN controller, use the **config ap secondary-base** command. The Cisco lightweight access point associates with this Cisco Wireless LAN controller for all network operation and in the event of a hardware reset.

```
config ap secondary-base controller_name Cisco_AP [controller_ip_address]
```

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	primary-base	Cisco lightweight access point secondary Cisco Wireless LAN controller.
	controller_name	Name of 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.

Defaults None.

Examples > config ap secondary-base SW_1 AP2

Related Commands

- show sysinfo
- config sysname
- config ap primary-base
- config ap tertiary-base

config ap sniff 802.11a

To enable or disable sniffing on the access point, use the **config ap sniff 802.11a** command.

When the sniffer feature is enabled on an access point, it starts sniffing the signal on the given channel. It captures and forwards all the packets to the remote computer that runs Omnippeek, Airoppeek, AirMagnet, or Wireshark. It includes information on timestamp, signal strength, packet size and so on.

Before an access point can act as a sniffer, a remote computer that runs one of the listed packet analysers must be set up so that it can receive packets sent by the access point. After the Airoppeek installation, copy the following .dll files to the location where airoppeek 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)

config ap sniff 802.11a {**enable** *channel* *server_IP_address* | **disable**} *Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Configure access point.
sniff	Sniffer command.
802.11a { enable disable }	Enable or disable sniffing.
<i>channel</i>	Channel to be sniffed.
<i>server_IP_address</i>	The IP address of the remote machine running Omnippeek, Airoppeek, AirMagnet, or Wireshark
<i>Cisco_AP</i>	Access point configured as the sniffer.

Defaults

Channel 36.

Examples

```
> config ap sniff 80211a enable 23 11.22.44.55 AP01
```

Related Commands

show ap config
config ap sniff 802.11b

config ap sniff 802.11b

To enable or disable sniffing on the access point, use the **config ap sniff 802.11b** command.

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. It includes information on timestamp, signal strength, packet size and so on.

Before an access point can act as a sniffer, a remote computer that runs one of the listed packet analysers must be set up so that it can receive packets sent by the access point. After the Airopeek installation, copy the following .dll files to the location where airopeek is installed.

- socket.dll file to the Plug-ins folder (for example, C:\Program Files\WildPackets\AiroPeek\Plugins)
- socketres.dll file to the PluginRes folder (for example, C:\Program Files\WildPackets\AiroPeek\1033\PluginRes)

config ap sniff 802.11b {**enable** *channel* *server_IP_address* | **disable**} *Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Configure access point.
sniff	Sniffer command.
802.11b { enable disable }	Enable or disable sniffing.
<i>channel</i>	Channel to be sniffed.
<i>server_IP_address</i>	The IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark
<i>Cisco_AP</i>	Access point configured as the sniffer.

Defaults

Channel 1.

Examples

```
> config ap sniff 80211b enable 23 11.22.44.55 AP01
```

Related Commands

show ap config
config ap sniff 802.11a

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*}

Syntax Description		
config		Configure parameters.
ap		Cisco lightweight access point.
static-ip		Configure Cisco lightweight access point static IP address settings.
{enable disable}		Configure the Cisco lightweight access point static IP address. Disable the Cisco lightweight access point static IP address. The access point uses DHCP to get the IP address.
<i>Cisco_AP</i>		Cisco lightweight access point name.
<i>ip_address</i>		Cisco lightweight access point IP address
<i>net_mask</i>		The Cisco lightweight access point network mask.
<i>gateway</i>		IP address of the Cisco lightweight access point gateway.

Defaults None.

Examples
 > 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

Use this command to set the time in seconds that the Cisco lightweight access point sends its DOT11 statistics to the Cisco Wireless LAN controller. A value of 0 (zero) means the Cisco lightweight access point will not send any DOT11 statistics. The acceptable range for the timer is from 0 to 65535 seconds, and the Cisco lightweight access point must be disabled to set this value.

config ap stats-timer *period Cisco_AP*

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	stats-timer	Cisco lightweight access point primary Cisco Wireless LAN controller.
	<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).

Examples > **config ap stats-timer 600 AP2**

Related Commands config ap disable

config ap syslog host global

To configure a global syslog server for all access points that join the controller, use the **config ap syslog host global** command.

config ap syslog host global *syslog_server_IP_address*



Note 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.

Syntax Description		
config		Configure parameters.
ap		Cisco lightweight access point.
syslog		System logs.
host		Remote host.
global		All Cisco lightweight access points.
<i>syslog_server_IP_address</i>		IP address of the syslog server.

Defaults 255.255.255.255.

Examples > **config ap syslog host global 255.255.255.255**

Related Commands

- config ap syslog host specific**
- show ap config global**
- show ap config general**

config ap syslog host specific

To configure a syslog server for a specific access point, use the **config ap syslog host specific** command.

```
config ap syslog host specific Cisco_AP syslog_server_IP_address
```

**Note**

By default, the syslog server IP address for each access point is 0.0.0.0, indicating that it is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	syslog	System logs.
	host	Remote host.
	specific	A single, specified Cisco access point.
	<i>syslog_server_IP_address</i>	IP address of the syslog server.

Defaults 0.0.0.0

Examples > config ap syslog host specific 0.0.0.0

Related Commands

config ap syslog host global

show ap config global

show ap config general

config ap {telnet | ssh}

To enable Telnet or SSH connectivity on an access point, use the **config ap {telnet | ssh}** command. The Cisco lightweight access point associates with this Cisco Wireless LAN controller for all network operation and in the event of a hardware reset.

config ap {telnet | ssh} {enable | disable} Cisco_AP

Syntax Description	
config	Configure parameters.
ap	Configure access point.
{telnet ssh}	- Enter telnet to configure Telnet connectivity on the access point. - Enter ssh to configure Secure Shell (SSH) connectivity on the access point.
{enable disable}	- Enter enable to enable Telnet or SSH connectivity on the access point. - Enter disable to disable Telnet or SSH connectivity on the access point.
<i>Cisco_AP</i>	Cisco access point name.

Defaults None.

Examples

```
> config ap telnet enable cisco_ap1
> config ap telnet disable cisco_ap1
> config ap ssh enable cisco_ap2
> config ap ssh disable cisco_ap2
```

Related Commands show ap config general

config ap tertiary-base

To set the Cisco lightweight access point tertiary Cisco Wireless LAN controller, use the **config ap tertiary-base** command. The Cisco lightweight access point associates with this Cisco Wireless LAN controller for all network operation and in the event of a hardware reset.

```
config ap tertiary-base controller_name Cisco_AP [controller_ip_address]
```

Syntax Description	config	Configure parameters.
	ap	Cisco lightweight access point.
	tertiary-base	Cisco lightweight access point tertiary Cisco Wireless LAN controller.
	controller_name	Name of 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.

Defaults None.

Examples > config ap tertiary-base SW_1 AP2

Related Commands

- show sysinfo
- config sysname
- config ap secondary-base
- config ap primary-base

config ap tftp-downgrade

This command is used to configure the settings used for downgrading a lightweight access point to an autonomous access point.

config ap tftp-downgrade (*tftp_ip_address*) (*image_filename*) (*ap_name*)

Syntax Description

<i>tftp_ip_address</i>	Specifies the IP address of the TFTP server.
<i>image_filename</i>	Specifies the filename of the access point image file on the TFTP server.
<i>ap_name</i>	Specifies the access point name.

Defaults

None.

Examples

```
> config ap tftp-downgrade 10.0.23.8 1238.tar ap1240_102301
```

Related Commands

show running-config
show version

config ap wlan

To enable or disable wireless LAN override for a Cisco lightweight access point radio, and to add or delete wireless LANs to or from a Cisco lightweight access point radio, as described in the related product guide, use the **config ap wlan** command.

config ap wlan {add | delete | enable | disable} {802.11a | 802.11b} wlan_id Cisco_AP

Syntax Description	
config	Configure parameters.
ap	Cisco lightweight access point.
wlan	Reset command.
{add delete enable disable}	- Add or delete a wireless LAN on an access point. (Cisco lightweight access point must have wireless LAN override enabled to add or delete a wireless LAN.) - Enable or disable per access point wireless LAN override on an access point.
{802.11a 802.11b}	Select 802.11a or 802.11b/g radio.
<i>wlan_id</i>	Optional Cisco Wireless LAN controller ID assigned to a wireless LAN.
<i>Cisco_AP</i>	Cisco lightweight access point name.

Defaults None.

Examples

To enable wireless LAN override on the AP03 802.11a radio:

```
> config ap wlan enable 802.11a AP03
```

To add wireless LAN ID 1 on the AP03 802.11a radio:

```
> config ap wlan add 802.11a 1 AP03
```

To delete wireless LAN ID 1 from the AP03 802.11a radio:

```
> config ap wlan delete 802.11a AP03
```

To disable wireless LAN override on the AP03 802.11a radio:

```
> config ap wlan disable 802.11a AP03
```

Related Commands `show ap wlan`

config ap username

To assign a username and password to access either a specific access point or all access points, use this command:

```
config ap username user_id password passwd [all | ap_name]
```

Syntax Description

username	Configures the access point's administrator username.
<i>user_id</i>	Specifies the administrator username.
password	Configures the access point's administrator password.
<i>passwd</i>	Specifies the administrator password.
all	Configures all
<i>ap_name</i>	Specifies the name of a specific access point.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

To assign a username and password to a specific access point enter a command similar to the following:

```
config ap username jack password blue 1a204
```

To assign the same username and password to all access points enter a command similar to the following:

```
config ap username jack password blue all
```

Related Commands

None.

config auth-list add

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

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

Syntax Description	config auth-list	Command action.
	add	Create an authorized access point entry.
	mic	Access point has manufacture installed certificate.
	ssc	Access point has self-signed certificate.
	AP_MAC	MAC address of a Cisco lightweight access point.
	AP_key	A key hash value equal to 20 bytes or 40 digits.

Defaults None.

Examples > 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	config auth-list	Command action.
	ap-policy	Create an authorized access point entry.
	authorize-ap {enable disable}	Enable or disable access point authorization.
	ssc {enable disable}	Enable or disable access point with self-signed certificate to connect.

Defaults None.

Examples

```
> config auth-list ap-policy authorize-ap enable
> config auth-list ap-policy ssc disable
```

Related Commands

```
config auth-list add
config auth-list delete
```

config auth-list delete

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

```
config auth-list delete AP_MAC
```

Syntax Description	config auth-list	Command action.
	delete	Delete an access point entry.
	AP_MAC	MAC address of a Cisco lightweight access point.

Defaults None.

Examples > config auth-list delete 00:0b:85:02:0d:20

Related Commands config auth-list add
 config auth-list ap-policy

config boot

Each Cisco Wireless LAN controller can boot off the primary, last-loaded OS image or boot off the backup, earlier-loaded OS image. To change a Cisco Wireless LAN controller boot option, use the **config boot** command.

config boot {primary | backup}

Syntax Description	config boot	Configure boot option.
	{primary backup}	Set the primary image or backup image as active.

Defaults	primary

Examples	> config boot primary
	> config boot backup

Related Commands	show boot

config cdp timer

This command is used to configure the CDP maximum hold timer.

config cdp timer *seconds*

Syntax Description	<i>seconds</i>	Specifies the maximum hold timer value (5 to 254 seconds).

Defaults	This command has no defaults.	

Command History	Release	Modification
	4.1	This command was introduced.

Examples	> config cdp timer 150	

Related Commands	None.	

config certificate

To configure SSL certificates, use the **config certificate** command.

config certificate {generate {webadmin | webauth} | compatibility {on | off}}

Syntax Description	config certificate	Command action.
	generate {webadmin webauth}	Generates a new web administration certificate or a new web authentication certificate.
	compatibility {on off}	Enables or disables compatibility mode for inter-Cisco Wireless LAN controller ipsec

Defaults	None.

Examples

```
> config certificate generate webadmin

Creating a certificate may take some time. Do you wish to continue? (y/n)

> config certificate compatibility
```

Related Commands

```
show certificate summary
show certificate compatibility
```

config certificate generate webadmin

To generate a new certificate, use the **config certificate generate webadmin** command.

config certificate generate webadmin

Syntax Description

config certificate	Command action.
generate webadmin	Generates a new web administration certificate.

Defaults

None.

Examples

```
> config certificate generate webadmin
```

Creating a certificate may take some time. Do you wish to continue? (y/n)

Related Commands

show certificate summary
show certificate compatibility

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 Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> config client ccx clear-reports 172.19.28.40
```

Related Commands

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

config client ccx clear-results

To clear the test results on the controller, use the **config client ccx clear-results** command.

config client ccx clear-results *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> config client deauthenticate 172.19.28.40
```

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 send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

config client ccx default-gw-ping

To send a request to the client to perform the default gateway ping test, use the **config client ccx default-gw-ping** command.

config client ccx default-gw-ping *client_mac_address*



Note This test does not require the client to use the diagnostic channel.

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> config client ccx default-gw-ping 00:E0:77:31:A3:55
```

Related Commands

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

config client ccx dhcp-test

To send a request to the client to perform the DHCP test, use the **config client ccx dhcp-test** command.

config client ccx dhcp-test *client_mac_address*



Note This test does not require the client to use the diagnostic channel.

Syntax Description

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

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> config client ccx dhcp-test 00:E0:77:31:A3:55
```

Related Commands

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

config client ccx dns-ping

To send a request to the client to perform the DNS server IP address ping test, use the **config client ccx dns-ping** command.

config client ccx dns-ping *client_mac_address*



Note This test does not require the client to use the diagnostic channel.

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> config client ccx dns-ping 00:E0:77:31:A3:55
```

Related Commands

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

config client ccx dns-resolve

To send a request to the client to perform the DNS name resolution test to the specified host name, use the **config client ccx dns-resolve** command.

config client ccx dns-resolve *client_mac_address* *host_name*



Note This test does not require the client to use the diagnostic channel.

Syntax Description

<i>client_mac_address</i>	Specifies the MAC address of the client.
<i>host_name</i>	Specifies the host name of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> config client ccx dns resolve 00:E0:77:31:A3:55 host_name
```

Related Commands

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

config client ccx get-client-capability

To send a request to the client to send its capability information, use the **config client ccx get-client-capability** command.

config client ccx get-client-capability *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> 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 Specifies the MAC address of the client.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples	> config client ccx get-manufacturer-info 172.19.28.40

Related Commands	config client ccx get-profiles
	config client ccx get-operating-parameters
	config client ccx get-client-capability
	config client ccx clear-reports
	show client ccx profiles
	show client ccx operating-parameters
	show client ccx manufacturer-info
	show client ccx client-capability
	config client ccx stats-request
	show client ccx stats-report

config client ccx get-operating-parameters

To send a request to the client to send its current operating parameters, use the **config client ccx get-operating-parameters** command.

config client ccx get-operating-parameters *client_mac_address*

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

Defaults	This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples	> config client ccx get-operating-parameters 172.19.28.40

Related Commands	config client ccx get-profiles
	config client ccx get-manufacturer-info
	config client ccx get-client-capability
	config client ccx clear-reports
	show client ccx profiles
	show client ccx operating-parameters
	show client ccx manufacturer-info
	show client ccx client-capability
	config client ccx stats-request
	show client ccx stats-report

config client ccx get-profiles

To send a request to the client to send its profiles, use the **config client ccx get-profiles** command.

config client ccx get-profiles *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> config client ccx get-profiles 172.19.28.40
```

Related Commands

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

config client ccx log-request

To configure a Cisco client extension (CCX) log request for a specified client device, use the **config client CCX log-request** command.

config client ccx log-request *log_type* [**roam** | **rsna** | **syslog**] *client_mac_address*

Syntax Description	roam	Specifies the request to specify the client CCX roaming log.
	rsna	Specifies the request to specify the client CCX RSNA log.
	syslog	Specifies the request to specify the client CCX system log.
	<i>client_mac_address</i>	Specifies the MAC address of the client.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

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

Tue Oct 05 13:05:21 2006
  SysLog Response LogID=1: Status=Successful
  Event Timestamp=121212121212
  Client SysLog = 'This is a test syslog 2'
  Event Timestamp=121212121212
  Client SysLog = 'This is a test syslog 1'
Tue Oct 05 13:04:04 2006
  SysLog Request LogID=1

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

Thu Jun 22 11:55:14 2006
  Roaming Response LogID=20: Status=Successful
  Event Timestamp=121212121212
  Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
  Transition Time=100(ms)
  Transition Reason: Unspecified Transition Result: Success
Thu Jun 22 11:55:04 2006
  Roaming Request LogID=20
Thu Jun 22 11:54:54 2006
  Roaming Response LogID=19: Status=Successful
  Event Timestamp=121212121212
  Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
  Transition Time=100(ms)
  Transition Reason: Unspecified Transition Result: Success
Thu Jun 22 11:54:33 2006  Roaming Request LogID=19
```

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

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

Related Commands

show client ccx log-response

config client ccx send-message

To send a message to the client, use the **config client ccx send-message** command.

config client ccx send-message *client_mac_address message_id*

Syntax Description

<i>client_mac_address</i>	Specifies the MAC address of the client.
<i>message_type</i>	Involves one of the following: • 1—The SSID is invalid. • 2—The network settings are invalide • 3—There is a WLAN credibility mismatch. • 4—The user credentials are incorrect. • 5—Please call support. • 6—The problem is resolved. • 7—The problem has not been resolved. • 8—Please try again later. • 9—Please correct the indicated problem. • 10—Troubleshooting is refused by the network. • 11—Retrieving client reports. • 12—Retrieving client logs. • 13—Retrieval complete. • 14—Beginning association test. • 15—Beginning DHCP test. • 16—Beginning network connectivitiy test. • 17—Beginning DNS ping test. • 18—Beginning name resolution test. • 19—Beginning 802.1X authentication test. • 20—Redirecting client to a specific profile. • 21—Test complete. • 22—Test passed. • 23—Test failed. • 24—Cancel diagnostic channel operation or select a WLAN profile to resume normal operation. • 25—Log retrieval refused by the client. • 26—Client report retrieval refused by the client. • 27—Test request refused by the client. • 28—Invalid network (IP) setting. • 29—There is a known outage or problem with the network. • 30—Scheduled maintenance period. • 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

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> config client ccx send-message 172.19.28.40 user-action-required
```

Related Commands

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

config client ccx stats-request

To send a request for statistics, use the **config client ccx stats-request** command.

config client ccx stats-request *measurement_duration stats_name [dot11 | security]*
client_mac_address

Syntax Description

<i>duration</i>	Specifies the measurement duration in seconds.
dot11	Specifies dot11 counters.
security	Specifies security counters.
<i>client_mac_address</i>	Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

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

Measurement duration = 1

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

Related Commands

show client ccx stats-report

config client ccx test-abort

To send a request to the client to abort the current test, use the **config client ccx test-abort** command.



Note Only one test can be pending at a time.

config client ccx test-abort *client_mac_address*

Syntax Description

client_mac_address Specifies the MAC address of the client.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> config client ccx test-abort 11:11:11:11:11:11
```

Related Commands

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

config client ccx test-association

To send a request to the client to perform the association test, use the **config client ccx test-association** command.

config client ccx test-association *client_mac_address* *ssid* *bssid* { **802.11a** | **802.11b** | **802.11g** } *channel*

Syntax Description

<i>client_mac_address</i>	Specifies the MAC address of the client.
<i>ssid</i>	Network name.
<i>bssid</i>	Basic ssid.
802.11a 802.11b 802.11g	802.11a, 802.11b, or 802.11g setting.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> config client ccx test-association 00:E0:77:31:A3:55 ssid bssid 802.11a
```

Related Commands

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

config client ccx test-dot1x

To send a request to the client to perform the 802.1x test, use the **config client ccx test-dot1x** command.

```
config client ccx test-dot1x client_mac_address profile_id bssid {802.11a | 802.11b | 802.11g}
channel
```

Syntax Description

<i>client_mac_address</i>	Specifies the MAC address of the client.
<i>profile_id</i>	Specifies the test profile name.
<i>bssid</i>	Basic ssid.
802.11a 802.11b 802.11g	802.11a, 802.11b, or 802.11g setting.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> 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>	Specifies the MAC address of the client.
	<i>profile_id</i>	Specifies the test profile name.
	Note	The <i>profile_id</i> should be from one of the client profiles for which client reporting is enabled.

Defaults This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples > config client ccx test-dot1 11:11:11:11:11:11 profile_01

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

config client deauthenticate

To disconnect a client, use the **config client deauthenticate** command.

config client deauthenticate *MAC*

Syntax Description	config	Configure parameters.
	client	Network client.
	deauthenticate	Deauthenticate command.
	<i>MAC</i>	Client MAC address.

Defaults None.

Examples

```
> config client deauthenticate 11:11:11:11:11:11
```

Related Commands

- show client summary
- show client detail

config client location-calibration

This command is used to configure link aggregation.

config client location-calibration [**enable** mac_address interval | **disable** mac_address]

Syntax Description

enable	Specifies that client location calibration is enabled.
disable	Specifies that client location calibration is disabled.
<i>mac_address</i>	Specifies the MAC address of the client.
<i>interval</i>	Specifies the measurement interval in seconds.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> config client location-calibration enable 37:15:86:2a:Bc:cf 45
```

Related Commands

show client location-calibration summary

config country

To configure the controller's country code, use the **config country** command. Use the **show country** command to display a list of supported countries.

config country *country_code*



Note

Cisco Wireless LAN controllers must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. Refer to the related product guide for the most recent country codes and regulatory domains.

Syntax Description

config	Configure parameters.
country	Set this Cisco Wireless LAN controller to comply with selected country's regulations.
<i>country_code</i>	A two-letter or three-letter country code.

Defaults

us (country code of the United States of America).

Examples

```
> config country DE
```

Related Commands

show country

config custom-web ext-webauth-mode

To configure external URL web-based client authorization for the custom-web authentication page, use the **config custom-web ext-webauth-mode** command.

```
config custom-web ext-webauth-mode {enable | disable}
```

Syntax Description	config custom-web	Command action.
	ext-webauth-mode {enable disable}	Enable or disable external URL web-based client authorization.

Defaults	None.

Examples	> config custom-web ext-webauth-mode enable

Related Commands	config custom-web redirectUrl
	config custom-web weblogo
	config custom-web webmessage
	config custom-web webtitle
	config custom-web ext-webauth-url
	show custom-web

config custom-web ext-webauth-url

To configure the complete external web authentication URL for the custom-web authentication page, use the **config custom-web ext-webauth-url** command.

config custom-web ext-webauth-url *URL*

Syntax Description

config custom-web	Command action.
ext-webauth-url <i>URL</i>	Set the complete external web authentication URL used for web-based client authorization.

Defaults

None.

Examples

```
> config custom-web ext-webauth-url http://www.AuthorizationURL.com/
```

Related Commands

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

config custom-web ext-webserver

To configure an external web server, use the **config custom-web ext-webserver** command.

config custom-web ext-webserver {**add** *index* *IP_address* | **delete** *index*}

Syntax Description	config custom-web	Command action.
	ext-webserver	The URL used for web-based client authorization.
	{add delete}	Add or delete an external web server.
	<i>index</i>	Index of the external web server in the list of external web server. Must be a number between 1 and 20.
	<i>IP_address</i>	The IP address of the external web server.

Defaults	None.

Examples	> config custom-web ext-webserver add 2 192.23.32.19

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

config custom-web redirectUrl

To configure the redirect URL for the custom-web authentication page, use the **config custom-web redirectUrl** command.

config custom-web redirectUrl *URL*

Syntax Description	config custom-web	Command action.
	redirectUrl <i>URL</i>	Set the redirect URL to the specified address.

Defaults	None.

Examples	<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 weblogo

To configure the web authentication logo for the custom-web authentication page, use the **config custom-web weblogo** command.

```
config custom-web weblogo {enable | disable}
```

Syntax Description	config custom-web	Command action.
	weblogo {enable disable}	Enable or disable the web authentication logo.

Defaults	None.

Examples	> config custom-web weblogo enable

Related Commands	config custom-web redirectUrl
	config custom-web webmessage
	config custom-web webtitle
	config custom-web ext-webauth-mode
	config custom-web ext-webauth-url
	show custom-web

config custom-web webmessage

To configure the custom web authentication message text for the custom-web authentication page, use the **config custom-web webmessage** command.

config custom-web webmessage *message*

Syntax Description

config custom-web	Command action.
webmessage <i>message</i>	Set custom message text for web authentication.

Defaults

None.

Examples

```
> config custom-web webmessage Thisistheplace
```

Related Commands

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

config custom-web webtitle

To configure the web authentication title text for the custom-web authentication page, use the **config custom-web webtitle** command.

config custom-web webtitle *title*

Syntax Description	config custom-web	Command action.
	webtitle <i>title</i>	Set the custom title text for web authentication.

Defaults	None.

Examples	> 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. Use the **show database** command to display local database configuration.

config database size *count*

Syntax Description	config database size	Command action.
	<i>count</i>	A database size value between 512 and 2040

Defaults	None.

Examples	Configures the dhcp lease for scope 003. > config database size 1024

Related Commands	show database

config dhcp

To configure the internal DHCP, use the **config dhcp** command. Use the show dhcp command to display the internal DHCP configuration.

```
config dhcp {address-pool scope start end | create-scope scope |
  default-router scope router_1 [router_2] [router_3] | delete-scope scope | disable scope |
  dns-servers scope dns1 [dns2] [dns3] | domain scope domain |
  enable scope | lease scope lease_duration |
  netbios-name-server scope wins1 [wins2] [wins3] |
  network scope network netmask}
```

Syntax	Description
config dhcp	Command action.
address-pool <i>scope start end</i>	Configure an address range to allocate. You must specify the scope name and the first and last addresses of the address range.
create-scope <i>name</i>	Create a new dhcp scope. You must specify the scope name.
default-router <i>scope router_1 [router_2] [router_3]</i>	Configure the default routers for the specified scope and specify the IP address of a router. Optionally, you can specify the IP addresses of secondary and tertiary routers.
delete-scope <i>scope</i>	Delete the specified DHCP scope.
disable <i>scope</i>	Disable the specified DHCP scope.
dns-servers <i>scope dns1 [dns2] [dns3]</i>	Configure the name servers for the given scope. You must also specify at least one name server. Optionally, you can specify secondary and tertiary name servers.
domain <i>scope domain</i>	Configure the DNS domain name. You must specify the scope and domain names.
enable <i>scope</i>	Enable the specified dhcp scope.
lease <i>scope lease_duration</i>	Configure the lease duration (in seconds) for the specified scope.
netbios-name-server <i>scope wins1 [wins2] [wins3]</i>	Configure the netbios name servers. You must specify the scope name and the IP address of a name server. Optionally, you can specify the IP addresses of secondary and tertiary name servers.
network <i>scope network netmask</i>	Configure the network and netmask. You must specify the scope name, the network address, and the network mask.

Defaults

None.

Examples

Configures the DHCP lease for the scope 003.

```
> config dhcp lease 003
```

Related Commands

show dhcp

config dhcp proxy

To specify the level at which DHCP packets are modified, use the **config dhcp proxy** command. Use the **show dhcp proxy** command to display the status of DHCP proxy handling.

```
config dhcp proxy {enable | disable}
```

Syntax Description	config dhcp proxy {enable disable}	Command action.
		- Enter enable to allow the controller to modify the DHCP packets without limit. - Enter disable to reduce DHCP packet modification to the level of a relay.
Defaults	Enabled.	
Examples	> config dhcp proxy disable	
Related Commands	show dhcp proxy	

config exclusionlist

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

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

Syntax Description	config exclusionlist	Configure the exclusion list.
	{add delete description}	- Enter add to create a local exclusion-list entry. - Enter delete to delete a local exclusion-list entry. - Enter description to set the description for an exclusion-list entry.
	MAC	MAC address of the local Excluded entry.
	[description]	[Optional] The description, up to 32 characters, for an excluded entry.

Defaults None.

Examples

```
> config exclusionlist add xx:xx:xx:xx:xx:xx lab
> config exclusionlist delete xx:xx:xx:xx:xx:xx lab
```

Related Commands show exclusionlist

Configure Interface Commands

Use the **config interface** commands to configure interface commands.

config guest-lan

To enable or disable a wired guest LAN, use the **config guest-lan** command.

config guest-lan {enable | disable} *guest_lan_id*



Note To delete a wired guest LAN, use the **config guest-lan delete** *guest_lan_id*.

Syntax Description

config	Command action.
guest-lan	Configure the guest LAN.
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Defaults

None.

Examples

```
> config guest-lan enable 1
```

Related Commands

config interface guest-lan, config guest-lan create

config guest-lan create

To create a wired LAN for wired client traffic and associate it to an interface, use the **config guest-lan create** command.

```
config guest-lan create guest_lan_id interface_name
```



Note To delete a wired guest LAN, use the **config guest-lan delete** *guest_lan_id*.

Syntax Description

config	Command action.
guest-lan	Configure the guest LAN.
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
<i>interface_name</i>	Interface name

Defaults

None.

Examples

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

Related Commands

```
config interface guest-lan
```

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

To redirect guest users to an external server before accessing the web login page, use the **config guest-lan custom-web ext-webauth-url** command to specify the URL of the external server.

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

Syntax	Description
config	Command action.
guest-lan	Configure the guest LAN.
custom-web	Customized web login page for wired guest users.
<i>ext_web_url</i>	Indicates the URL for the external server
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Defaults None.

Examples > **config guest-lan custom-web ext-webauth-url http://www.AuthorizationURL.com/ 1**

Related Commands

- config guest-lan**
- config guest-lan create**
- config guest-lan custom-web login_page**

config guest-lan custom-web global disable

To use a guest-LAN specific custom web configuration rather than a global custom web configuration, use the **config guest-lan custom-web global disable** command.

config guest-lan custom-web global disable *guest_lan_id*



Note 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.

Syntax Description

config	Command action.
guest-lan	Configure the guest LAN.
custom-web global disable	Indicates the disabling of the global custom web configuration.
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Defaults

None.

Examples

```
> config guest-lan custom-web global disable 1
```

Related Commands

config guest-lan
config guest-lan create
config guest-lan custom-web ext-webauth-url
config guest-lan custom-web login_page
config guest-lan custom-web webauth-type {internal | customized | external}

config guest-lan custom-web login_page

To enable wired guest users to log into a customized web login page, use the **config guest-lan custom-web login_page** command to specify the filename of the web login page and the wired LAN for which it should display.

config guest-lan custom-web login_page *page_name guest_lan_id*

Syntax Description	config	Command action.
	guest-lan	Configure the guest LAN.
	custom-web login_page	Customized web login page for wired guest users.
	<i>page_name</i>	Indicates the name of the customized web login page.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Defaults None.

Examples

```
> config guest-lan custom-web login_page custompage1 1
```

Related Commands

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

config guest-lan custom-web webauth-type

To define the web login page for wired guest users, use the **config guest-lan custom-web webauth-type** command.

```
config guest-lan custom-web webauth-type {internal | customized | external} guest_lan_id
```

Syntax Description	config	Command action.
	guest-lan	Configure the guest LAN.
	custom-web webauth-type	Indicates the type of web authorization page.
	internal	Displays the default web login page for the controller. This is the default value.
	customized	Displays the custom web login page that was previously configured.
	external	Redirects users to the URL that was previously configured.
	guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).

Defaults Internal.

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

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

config guest-lan ingress-interface

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

config guest-lan ingress-interface *guest_lan_id* *interface_name*

Syntax Description	config interface	Command action.
	guest-lan	Configure the guest LAN.
	ingress-interface	Provides a path between the wired guest client and the controller by way of the Layer 2 access switch.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
	<i>interface_name</i>	Interface name

Defaults	None.

Examples	> config interface ingress-interface 1 guest01

Related Commands	config interface guest-lan config guest-lan create

config guest-lan interface

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

```
config guest-lan interface guest_lan_id interface_name
```

Syntax Description	config	Command action.
	guest-lan	Configure the guest LAN.
	interface	Provides a path between the wired guest client and the controller by way of the Layer 2 access switch.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
	<i>interface_name</i>	Interface name

Defaults None.

Examples > config guest-lan interface 1 guest01

Related Commands config ingress-interface guest-lan
config guest-lan create

config guest-lan nac

To enable or disable NAC out-of-band support for a guest LAN, enter this command:

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

Syntax Description	config	Command action.
	guest-lan	Configure the guest LAN.
	nac	NAC out-of-band support.
	enable disable	Enable or disable NAC out-of-band support.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Defaults	None

Examples	<pre>>config guest-lan nac enable 3</pre>

Related Commands	<code>config guest-lan create</code>

config guest-lan security

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

```
config guest-lan security { web-auth enable guest_lan_id | web-passthrough enable  
                           guest_lan_id }
```

Syntax Description

config	Command action.
guest-lan	Configure the guest LAN.
security	Indicates the security policy for the wired guest LAN.
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
web-auth enable	Enable web authentication.
web-passthrough enable	Enable the web captive portal with no authentication required.

Defaults

Web authentication.

Examples

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

Related Commands

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

config hreap group (add or delete)

To add or delete a hybrid-REAP group, use the **config hreap group** command.

```
config hreap group group_name {add | delete}
```

Syntax Description	config hreap group	Command action
	<i>group_name</i>	Enter group name.
	{ add delete }	Specify whether you want to add or delete a group.

Defaults	None.

Examples	> config hreap group 192.12.1.2 add

Related Commands	config hreap group <i>group_name</i> radius server config hreap group <i>group_name</i> ap show hreap group summary show hreap group detail

config hreap group (RADIUS server)

To configure a primary or secondary RADIUS server for the hybrid-REAP group, use the **config hreap group** *group_name* **radius server** command.

```
config hreap group group_name radius server {add | delete} {primary | secondary}
server_index
```

Syntax Description	config hreap group	Command action
	group_name	Enter group name.
	radius server	RADIUS server
	{add delete}	Specify whether you want to add or delete a group.
	{primary secondary}	Specify primary or secondary server index
	server_index	Server index

Defaults None.

Examples > config hreap group 192.12.1.2 radius server add primary 1

Related Commands

config hreap group *group_name*
config hreap group *group_name* ap
show hreap group summary
show hreap group detail

config hreap group (ap)

To add an access point to the hybrid-REAP group, use the **config hreap group** *group_name* **ap** command.

```
config hreap group group_name ap {add | delete} ap_mac
```

Syntax Description	config hreap group	Command action
	<i>group_name</i>	Enter group name.
	{ add delete }	Specify whether you want to add or delete a group.
	<i>ap_mac</i>	MAC address of the access point

Defaults None.

Examples

```
> config hreap group 192.12.1.2 ap add 00:E0:77:31:A3:55
```

Related Commands

```
config hreap group group_name
config hreap group group_name radius server
show hreap group summary
show hreap group detail
```

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 }
```



Note For a Cisco 2100 series wireless LAN controller, you must configure a pre-authentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any pre-authentication ACL for Cisco 4400 series wireless LAN controllers.

Syntax Description	config interface acl	Command action
	ap-manager	Configures the access point manager interface.
	management	Configures the management interface.
	interface_name	Enter interface name.
	{ ACL none }	Specify an ACL name up to 32 alphanumeric characters or enter none .

Defaults None.

Examples > config interface acl management none

Related Commands show interface

config interface address

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

```

config interface address
  {ap-manager IP_address netmask gateway |
management IP_address netmask gateway |
service-port IP_address netmask |
virtual IP_address |
interface-name interface-name IP_address netmask gateway}

```

Syntax Description

ap-manager	Specifies the access point manager interface.
management	Specifies the management interface.
service-port	Specifies the out-of-band service port interface.
virtual	Specifies the virtual gateway interface.
interface-name	Specifies the interface identified by the <i>interface-name</i> parameter.
<i>interface-name</i>	Specifies the interface name.
<i>IP_address</i>	Specifies the IP address.
<i>netmask</i>	Specifies the network mask.
<i>gateway</i>	Specifies the IP address of the gateway.

Defaults

None.

Examples

```
> config interface address ap-manager 10.109.15.7 255.255.0.0 10.109.15.1
```

Related Commands

show interface

config interface ap-manager

To enable or disable access point manager features on a dynamic interface, use the **config interface ap-manager** command.

```
config interface ap-manager interface_name {enable | disable}
```

Syntax Description	config interface	Command action.
	ap-manager	Configures access point manager features on a dynamic interface.
	interface_name	Interface's name.
	{enable disable}	Enable or disable access point manager features on a dynamic interface.

Defaults	None.

Examples	> config interface ap-manager myinterface disable

Related Commands	show interface

config interface create

To create a dynamic interface (VLAN) for wired guest user access, use the **config interface create** command.

config interface create *interface_name* *vlan-id*

Syntax Description	config interface	Command action
	create	Create a new dynamic interface.
	<i>interface_name</i>	Interface's name.
	<i>vlan-id</i>	VLAN identifier.

Defaults	None.

Examples	> config interface create lab2 6

Related Commands	show interface

config interface delete

To delete a dynamic interface, use the **config interface delete** command.

config interface delete *interface-name*

Syntax Description	config interface	Command action.
	delete	Delete the specified dynamic interface.
	<i>interface-name</i>	Interface's name.

Defaults	None.

Examples	> config interface delete VLAN501

Related Commands	show interface

config interface dhcp

To configure DHCP options on an interface, use the **config interface dhcp** command.

```
config interface dhcp {
  ap-manager [primary dhcp_server secondary dhcp_server | option-82 [enable | disable] ] |
  management [primary dhcp_server secondary dhcp_server | option-82 [enable | disable] ] |
  service-port {enable | disable} |
  interface-name name [primary dhcp_server secondary dhcp_server | option-82 [enable |
  disable] ] }
```

Syntax Description		
ap-manager		Configures the access point manager interface.
server-1		Configures the primary DHCP server.
<i>dhcp_server</i>		Specifies the IP address of the server.
server-2		Configures the alternate DHCP server.
option-82		Configures DHCP option 43 on the interface.
enable		Enables the feature.
disable		Disables the feature.
management		Configures the management interface.
service-port		Enables or disables DHCP for the out-of-band service port.
interface-name		Enter the interface name and the primary DHCP server. Optionally, you can also enter the address of the alternate DHCP server.

Defaults None.

Examples

```
> config interface dhcp ap-manager server-1 10.21.15.01 server-2 10.21.15.25
> config interface dhcp ap-manager option-82 enable
> config interface dhcp service-port enable
```

Related Commands show interface

config interface guest-lan

To enable or disable the guest LAN VLAN, use the **config interface guest-lan** command.

```
config interface guest-lan interface_name {enable | disable}
```

Syntax Description	config interface	Command action.
	guest-lan	Configure the guest LAN.
	<i>interface_name</i>	Interface name.
	enable disable	Enable or disable the feature.

Defaults	None.

Examples	> config interface guest-lan myinterface enable

Related Commands	config guest-lan create

config interface hostname

To configure the DNS host name of the virtual gateway interface, use the **config interface hostname** command.

config interface hostname virtual *DNS_host*

Syntax Description	config interface	Command action.
	hostname	Configure the DNS host name
	virtual <i>DNS_host</i>	Configures the virtual gateway interface to use the specified virtual address of the fully qualified DNS name. (The Virtual Gateway IP Address is any fictitious, unassigned IP address, such as 1.1.1.1, to be used by Layer 3 security and mobility managers.)

Defaults None.

Examples > **config interface hostname virtual DNS_Host**

Related Commands show interface

config interface 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 interface_name primary_port {secondary_port}
```

Syntax Description

config interface port	Command action.
<i>interface_name</i>	Interface name
<i>primary_port</i> <i>{secondary_port}</i>	Interface’s primary or secondary physical port number.

Defaults

None.

Examples

```
> config interface port lab02 3
```

Related Commands

show interface, config interface create

config interface quarantine vlan

To configure a quarantine VLAN on any dynamic interface, use the **config interface quarantine vlan** command.

config interface quarantine vlan *interface-name* *vlan_id*

Syntax Description	config interface	Command action.
	quarantine vlan	Configure quarantine VLAN for this interface.
	<i>interface-name</i>	Interface's name.
	<i>vlan_id</i>	VLAN identifier.
	Note	Enter 0 to disable quarantine processing.

Defaults	None.

Examples	> config interface quarantine vlan quarantine 10

Related Commands	show interface

config interface vlan

To configure an interface’s VLAN identifier, use the **config interface vlan** command.

```
config interface vlan {ap-manager | management | interface-name} vlan
```

Syntax Description	config interface	Command action.
	vlan	Configure an interface’s VLAN identifier
	{ap-manager management interface-name}	- Enter ap-manager to configure the access point manager interface. - Enter management to configure the management interface. - Enter the interface’s name.
	interface-name	Interface’s name.
	vlan	VLAN identifier.

Defaults	None.

Examples	> config interface vlan management 01

Related Commands	show interface

config known ap

To configure a known Cisco lightweight access point, use the **config known ap** command.

config known ap {add | alert | delete} MAC

Syntax Description	
config	Configure parameters.
known ap	Known Cisco lightweight access point.
{add alert delete}	• Add a new known access point Entry. • Generate a trap upon detection of the access point. • Delete an existing known access point Entry.
MAC	MAC address of the known Cisco lightweight access point.

Defaults None.

Examples
 > **config known ap add ac:10:02:72:2f:bf 12**

Related Commands **config ap**

config lag

This command is used to enable or disable link aggregation (LAG).

config lag [**enable** | **disable**]

Syntax Description	enable	Specifies that link aggregation is enabled.
	disable	Specifies that link aggregation is disabled.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> config lag enable
```

Enabling LAG will map your current interfaces setting to LAG interface,
All dynamic AP Manager interfaces and Untagged interfaces will be deleted
All WLANs will be disabled and mapped to Mgmt interface
Are you sure you want to continue? (y/n)

You must now reboot for the settings to take effect.

```
> config lag disable
```

Disabling LAG will map all existing interfaces to port 1.
Are you sure you want to continue? (y/n)

You must now reboot for the settings to take effect.

Related Commands **show lag summary**

config ldap

To configure lightweight directory access protocol (LDAP) server settings, use the **config ldap** command.

config ldap {add | delete | disable | enable | retransmit-timeout} *index*

Syntax Description	add	Specifies that an LDAP server is being added.
	delete	Specifies that an LDAP server is being deleted.
	enable	Specifies that an LDAP serve is enabled.
	disable	Specifies that an LDAP server is disabled.
	retransmit-timeout	Changes the default retransmit timeout for an LDAP server.
	<i>index</i>	LDAP server index. Valid values are from 1 to 17.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples
 > **config ldap enable 10**

Related Commands

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

config ldap add

This command is used configure a lightweight directory access protocol (LDAP) server.

config lap add *index server_ip_address port user_base user_attr user_type*

Syntax Description

<i>index</i>	Specifies the LDAP server index.
<i>server_ip_address</i>	Specifies the IP address of the LDAP server.
<i>port</i>	Specifies the port.
<i>user_base</i>	Specifies the distinguished name for the subtree that contains all of the users.
<i>user_attr</i>	Specifies the attribute that contains the users name.
<i>user_type</i>	Specifies the objectType that identifies the user.

Defaults

This command has no defaults..

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> config ldap add 10 10.31.15.45 2 base_name attr_name type_name
```

Related Commands

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

config ldap simple-bind

To configure the local authentication bind method for the LDAP server, use the **config ldap simple-bind** command.

```
config ldap simple-bind {anonymous index | authenticated index username username password password}
```

Syntax Description

anonymous	Allows anonymous access to the LDAP server
<i>index</i>	Specifies the LDAP server index.
authenticated	Requires that a username and password be entered to secure access to the LDAP server.
username <i>username</i>	Username for authenticated bind method.
password <i>password</i>	Password for authenticated bind method.

Defaults

The default bind method is **anonymous**.

Examples

```
> config ldap simple-bind anonymous
```

Related Commands

[config ldap](#)
[config ldap add](#)
[show ldap summary](#)

config load-balancing

To change the state of the load-balancing feature, use the **config load-balancing** command.

```
config load-balancing {status {enable | disable} | window clients}
```

Syntax Description	config	Configure parameters.
	load-balancing	Configures aggressive load-balancing.
	status {enable disable}	Enable or disable the aggressive load balancing status.
	window clients	Set the aggressive load balancing client window with the number of clients from 0 to 20.

Defaults	Enabled

Examples	> config load-balancing enable

Related Commands	show load-balancing

config local-auth active-timeout

To specify the amount of time in which the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fails, enter this command:

config local-auth active-timeout *timeout*

Syntax Description	config	Configure parameters.
	local-auth	Configures local authentication.
	active-timeout	The amount of time in which the controller attempts to authenticate wireless clients using local EAP
	<i>timeout</i>	The timeout measured in seconds. Valid range is 1 to 3600.

Defaults This command has a default of 100 seconds.

Examples > **config local-auth active-timeout 500**

Related Commands **config local-auth eap-profile**
show local-auth config

config local-auth eap-profile

This command is used to configure local EAP authentication profiles.

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

Syntax Description

config	Configures parameters.
local-auth	Configures local authentication.
eap-profile	Configures a local EAP profile.
add	Specifies that an EAP profile or method is being added.
delete	Specifies that an EAP profile or method is being deleted.
cert-issuer	(For use with EAP-TLS, PEAP, or EAP-FAST with certificates) Specifies the issuer of the certificates that will be sent to the client. The supported certificate issuers are Cisco or a third-party vendor.
method	Configures an EAP profile method.
<i>method</i>	Specifies the EAP profile method name. The supported methods are leap, fast, tls, and peap.
<i>profile_name</i>	Specifies the EAP profile name (up to 63 alphanumeric characters). Do not include spaces within a profile name.
local-cert	(For use with EAP-FAST) Specifies whether the device certificate on the controller is required for authentication.
client-cert	(For use with EAP-FAST) Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.
peer-verify	Configures the peer certificate verification options.
ca-issuer	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the incoming certificate from the client is to be validated against the Certificate Authority (CA) certificates on the controller.
cn-verify	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates' CN on the controller.
date-valid	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.
enable	Specifies that the parameter is enabled.
disable	Specifies that the parameter is disabled.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

To create a local EAP profile named “FAST01,” enter this command:

```
> config local-auth eap-profile add FAST01
```

To add the EAP-FAST method to a local EAP profile, enter this command:

```
> config local-auth eap-profile method add fast FAST01
```

To specify Cisco as the issuer of the certificates that will be sent to the client for an EAP-FAST profile, enter this command:

```
> config local-auth eap-profile method fast cert-issuer cisco
```

To specify that the incoming certificate from the client be validated against the CA certificates on the controller, enter this command:

```
> config local-auth eap-profile method fast peer-verify ca-issuer enable
```

Related Commands

config local-auth method fast

show local-auth config

config local-auth method fast

This command is used to configure an EAP-FAST profile.

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

Syntax Description

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

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was released.

Examples

```
> config local-auth method fast anon-prov disable
> config local-auth method fast authority-id 0125631177
> config local-auth method fast pac-ttl 10
> config local-auth method fast server-key 210967Fa7D4A11AA
```

Related Commands

config local-auth eap-profile
show local-auth config

config local-auth user-credentials

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

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



Note

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

Syntax Description

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

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> config local-auth user-credentials local ldap
```

Related Commands

show local-auth config

config location

This command is used to configure a location-based system.

```
config location {802.11b monitor {enable | disable} Cisco_AP |
  algorithm {simple | rssi-average} |
  rssi-half-life [client | calibrating-client | tags | rogue-aps] seconds |
  expiry [client | calibrating-client | tags | rogue-aps] seconds }
```

Syntax	Description
802.11b monitor	Configures Location Optimized Monitor Mode (LOMM).
enable disable	Enable or disable an option.
<i>Cisco_AP</i>	The name of the Cisco access point.
algorithm	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	Configures the half life when averaging two RSSI readings.
expiry	Configures the timeout for RSSI values.
client	Specifies the parameter applies to client devices.
calibrating-client	Specifies the parameter is used for calibrating client devices.
tags	Specifies the parameter applies to radio frequency identification (RFID) tags.
rogue-aps	Specifies the parameter applies to rogue access points.
<i>seconds</i>	Specifies a time value (0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, 300 seconds).

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> config location algorithm simple
> config location expiry client 60
```

Related Commands show location

config location add

To create a new Cisco lightweight access point location, use the **config location add** command.

config location add *location* [*description*]

Syntax Description	config	Configure parameters.
	location	Cisco lightweight access point location.
	add	Add a location.
	<i>location</i>	Location name.
	[<i>description</i>]	(Optional) Location description.

Defaults	None.

Examples	> config location add warehouse

Related Commands	show location config location enable config location disable config location delete config location description config interlace-mapping

config location delete

To delete an existing Cisco lightweight access point location, use the **config location delete** command.

config location delete *location*

Syntax Description

config	Configure parameters.
location	Cisco lightweight access point location.
delete	Delete a location.
<i>location</i>	Location name.

Defaults

None.

Examples

```
> config location delete warehouse
```

Related Commands

show location
config location add
config location enable
config location disable
config location description
config interlace-mapping

config location description

To specify a description of a Cisco lightweight access point location, use the **config location description** command.

config location description *location_name description*

Syntax Description	config	Configure parameters.
	location	Cisco lightweight access point location.
	description	Description of a location.
	<i>location_name</i>	Location name.
	<i>description</i>	Location description.

Defaults	None.

Examples	> config location description warehouse bld02

Related Commands	show location config location add config location delete config location enable config location disable config interlace-mapping

config location disable

To disable Cisco lightweight access point location-based overrides, use the **config location disable** command.

config location disable

Syntax Description	config	Configure parameters.
	location	Cisco lightweight access point location.
	disable	Disable location-based overrides.

Defaults

None.

Examples

> **config location disable**

Related Commands

show location
config location add
config location delete
config location description
config interlace-mapping
config location enable

config location enable

To enable or disable Cisco lightweight access point location-based overrides, use the **config location enable** command.

config location enable

Syntax Description	config	Configure parameters.
	location	Cisco lightweight access point location.
	enable	Enable location-based overrides.

Defaults	None.

Examples	> config location enable

Related Commands	show location config location add config location delete config location description config interlace-mapping config location disable

config location interface-mapping

To add or delete a new Cisco lightweight access point location/wireless LAN/interface mapping, use the **config location interface-mapping** command.

```
config location interface-mapping {add location_name wlan_id interface_name |
delete location_name wlan_id}
```

Syntax Description	config	Configure parameters.
	location	Cisco lightweight access point location.
	interface-mapping	Add or delete location/wireless LAN/interface mapping.
	{add delete}	Add or delete a new location/wireless LAN/interface mapping.
	location_name	Location name.
	wlan_id	Wireless LAN Identifier between 1 and 16.
	interface_name	Interface's name.

Defaults None.

Examples > config location interface-mapping add warehouse 13

Related Commands

- show location
- config location add
- config location delete
- config location description
- config location

config logging buffered

To set the severity level for logging messages to the controller buffer, use the **config logging buffered** command.

config logging buffered *security_level*

Syntax Description	
config	Configure parameters.
logging	Syslog facility logging.
buffered	Controller buffer.
<i>security_level</i>	One of the following: - emergencies—Severity level 0 - alerts—Severity level 1 - critical—Severity level 2 - errors—Severity level 3 - warnings—Severity level 4 - notifications—Severity level 5 - informational—Severity level 6 - debugging—Severity level 7

Defaults None.

Examples > **config logging buffered 4**

Related Commands

- config logging syslog facility**
- config logging syslog level**
- show logging**

config logging console

To set the severity level for logging messages to the controller console, use the **config logging console** command.

config logging console *security_level*

Syntax Description

config	Configure parameters.
logging	Syslog facility logging.
console	Controller console.
<i>security_level</i>	One of the following: - emergencies—Severity level 0 - alerts—Severity level 1 - critical—Severity level 2 - errors—Severity level 3 - warnings—Severity level 4 - notifications—Severity level 5 - informational—Severity level 6 - debugging—Severity level 7

Defaults

None.

Examples

```
> config logging console 3
```

Related Commands

config logging syslog facility
config logging syslog level
show logging

config logging debug

To save debug messages to the controller buffer, the controller console, or a syslog server, use the **config logging debug** command.

config logging debug {buffered | console | syslog} {enable | disable}

Syntax Description		
config		Configure parameters.
logging		Syslog facility logging.
debug		Set debug message logging parameters.
buffered		Save debug messages to the controller buffer.
console		Save debug messages to the controller console.
syslog		Save debug messages to the syslog server.
{enable disable}		- Enter enable to enable logging of debug messages. - Enter disable to disable logging of debug messages.

Command Default

The **console** command is enabled,
The **buffered** and **syslog** commands are disabled.

Examples

```
>config logging debug console enable
```

Related Commands

show logging

config logging fileinfo

To cause the controller to include information about the source file in the message logs or to prevent the controller from displaying this information, use the **config logging fileinfo** command.

config logging fileinfo {enable | disable}

Syntax Description	config	Configure parameters.
	logging	Syslog facility logging.
	fileinfo	Information about the source file
	{enable disable}	- Enter enable to include information about the source file in the message logs. - Enter disable to prevent the controller from displaying information about the source file in the message logs.

Defaults None.

Examples > **config logging fileinfo enable**

Related Commands **show logging**

config logging procinfo

To cause the controller to include process information in the message logs or to prevent the controller from displaying this information, use the **config logging procinfo** command.

config logging procinfo {enable | disable}

Syntax Description	config	Configure parameters.
	logging	Syslog facility logging.
	procinfo	Process information.
	{enable disable}	- Enter enable to include process information in the message logs. - Enter disable to prevent the controller from displaying process information in the message logs.

Defaults None.

Examples > **config logging procinfo enable**

Related Commands show logging

config logging traceinfo

To cause the controller to include traceback information in the message logs or to prevent the controller from displaying this information, use the **config logging traceinfo** command.

config logging traceinfo { enable | disable }

Syntax Description	config	Configure parameters.
	logging	Syslog facility logging.
	traceinfo	Traceback information.
	{ enable disable }	- Enter enable to include traceback information in the message logs. - Enter disable to prevent the controller from displaying traceback information in the message logs.

Defaults	None.

Examples	> config logging traceinfo disable

Related Commands	show logging

config logging syslog host

To configure a remote host for sending syslog messages, use the **config logging syslog host** command.

config logging syslog host {*host_IP_address*}



Note To remove a remote host that was configured for sending syslog messages, enter this command:
config logging syslog host *host_IP_address* **delete**.

Syntax Description

config	Configure parameters.
logging	Syslog facility logging.
syslog	System logs.
host	Remote host.
<i>IP_address</i>	IP address for the remote host.

Defaults

None.

Examples

```
> config logging syslog host 10.92.125.51
```

Related Commands

config logging syslog facility
config logging syslog level
show logging

config logging syslog facility

To set the facility for outgoing syslog messages to the remote host, use the **config logging syslog facility** command.

config logging syslog facility *{facility_code}*

Syntax Description

config	Configure parameters.
logging	Syslog facility logging.
syslog	System logs.
facility	Syslog facility
<i>facility_code</i>	One of the following: • authorization—Authorization system. Facility level—4. • auth-private—Authorization system (private). Facility level—10. • cron—Cron/at facility. Facility level—9. • daemon—System daemons. Facility level—3. • ftp—FTP daemon. Facility level—11. • kern—Kernel. Facility level—0. • local0—Local use. Facility level—16. • local1—Local use. Facility level—17. • local2—Local use. Facility level—18. • local3—Local use. Facility level—19. • local4—Local use. Facility level—20. • local5—Local use. Facility level—21. • local6—Local use. Facility level—22. • local7—Local use. Facility level—23. • lpr—Line printer system. Facility level—6. • mail—Mail system. Facility level—2. • news—USENET news. Facility level—7. • sys12—System use. Facility level—12. • sys13—System use. Facility level—13. • sys14—System use. Facility level—14. • sys15—System use. Facility level—15. • syslog—The syslog itself. Facility level—5. • user—User process. Facility level—1. • uucp—Unix-to-Unix copy system. Facility level—8.

Defaults

None.

Examples

```
> config logging syslog facility authorization
```

Related Commands

```
config logging syslog host  
config logging syslog level  
show logging
```

config logging syslog level

To set the severity level for filtering syslog messages to the remote host, use the **config logging syslog level** command.

```
config logging syslog level {severity_level}
```

Syntax Description	config	Configure parameters.
	logging	Syslog facility logging.
	syslog	System logs.
	level	Syslog message severity level
	severity_level	One of the following: - emergencies—Severity level 0 - alerts—Severity level 1 - critical—Severity level 2 - errors—Severity level 3 - warnings—Severity level 4 - notifications—Severity level 5 - informational—Severity level 6 - debugging—Severity level 7

Defaults None.

Examples None.

Related Commands

config logging syslog host

config logging syslog facility

show logging

config loginsession close

To close all active telnet session(s), use the **config loginsession close** command.

```
config loginsession close {session_id | all}
```

Syntax Description	config	Configure parameters.
	loginsession close	Close specified telnet sessions.
	{session_id all}	Enter the ID of the session to close.
		Enter all to close all telnet sessions.

Defaults

None.

Examples

```
> config loginsession close all
```

Related Commands

[show loginsession](#)

Configure Macfilter Commands

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

config macfilter add

To create a MAC filter entry on the Cisco Wireless LAN controller, use the **config mac filter add** command. Use this command to add a client locally to a wireless LAN on the Cisco Wireless LAN controller. This filter bypasses the RADIUS authentication process.

```
config macfilter add MAC_address wlan_id [interface_name] [description] [IP address]
```

Syntax Description	MAC_address	Client MAC address.
	wlan_id	Wireless LAN Identifier to associate with. A zero value associates the entry with any wireless LAN.
	interface_name	Interface's name. Enter 0 to specify no interface.
	description	(Optional) Short description of the interface (up to 32 characters), in double quotes.
		Note Description is mandatory if IP address is specified.
	IP address	(Optional) Specifies the IP address of the local MAC filter database.

Defaults None.

Examples > 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 delete

Use to remove a local client from the Cisco Wireless LAN controller, use the **config macfilter delete** command.

config macfilter delete *MAC*

Syntax Description

config	Configure parameters.
macfilter	Local MAC address filter.
delete	Delete a client.
<i>MAC</i>	Client MAC address.

Defaults

None.

Examples

```
> config macfilter delete 11:11:11:11:11:11
```

```
Deleted user 111111111111
```

Related Commands

[show macfilter](#)

config macfilter description

Use to add a description to a MAC filter, use the **config macfilter description** command.

```
config macfilter description MAC [description]
```

Syntax Description	config	Configure parameters.
	macfilter	Local MAC address filter.
	description	Sets the description for a mac filter.
	MAC	Client MAC address.
	[description]	Optional description within double quotes (up to 32 characters).

Defaults	None.

Examples	> config macfilter description 11:11:11:11:11:11 "MAC Filter 01"

Related Commands	show macfilter

config macfilter interface

Use to create a MAC filter client interface, use the **config macfilter interface** command.

config macfilter interface *MAC interface*

Syntax Description	config	Configure parameters.
	macfilter	Local MAC address filter.
	interface	Create interface.
	<i>MAC</i>	Client MAC address.
	<i>interface</i>	Interface's name. A value of zero is equivalent to no name.

Defaults	None.

Examples	> config macfilter interface 11:11:11:11:11:11 Lab01

Related Commands	show macfilter

config macfilter ip-address

To assign an IP address to an existing MAC filter entry, if one was not assigned using the **config macfilter add** command, use the following command:

```
config macfilter ip-address MAC_address IP address
```

Syntax Description	MAC_address	Client MAC address.
	IP address	Specifies the IP address for a specific MAC address in the local MAC filter database.

Defaults	None.

Examples	<code>config macfilter ip-address 00:E0:77:31:A3:55 10.92.125.51</code>

Related Commands	show macfilter config macfilter add

config macfilter mac-delimiter

To set the MAC delimiter (colon, hyphen, none, and single-hyphen) for MAC addresses sent to RADIUS servers, use the **config macfilter mac-delimiter** command.

config macfilter mac-delimiter { none | colon | hyphen | single-hyphen }

Syntax Description

config	Configure parameters.
macfilter	Local MAC address filter.
mac-delimiter	Configure MAC address format for RADIUS servers.
{ none colon hyphen single-hyphen }	- Enter none to disable delimiters (for example, xxxxxxxxxx). - Enter colon to set the delimiter to colon (for example, xx:xx:xx:xx:xx:xx). - Enter hyphen to set the delimiter to hyphen (for example, xx-xx-xx-xx-xx-xx). - Enter single-hyphen to set the delimiter to a single hyphen (for example, xxxxxx-xxxxxx).

Defaults

None.

Examples

To have OS send MAC address to RADIUS servers in the form aa:bb:cc:dd:ee:ff:

```
> config macfilter mac-delimiter colon
```

To have OS send MAC address to RADIUS servers in the form aa-bb-cc-dd-ee-ff:

```
> config macfilter mac-delimiter hyphen
```

To have OS send MAC address to RADIUS servers in the form aabbccddeeff:

```
> config macfilter mac-delimiter none
```

Related Commands

[show macfilter](#)

config macfilter radius-compat

Use to configure the Cisco Wireless LAN controller for compatibility with selected RADIUS servers.

```
config macfilter radius-compat { cisco | free | other }
```

Syntax Description	config	Configure parameters.
	macfilter	Local MAC address filter.
	radius-compat	Compatibility with selected RADIUS server.
	{ cisco free other }	- Enter cisco to configure Cisco ACS Compatibility mode (password is the MAC address of the server). - Enter free to configure Free RADIUS Server Compatibility mode (password is secret). - Enter other to configure for other server behaviors (no password necessary).

Defaults Other.

Examples > config macfilter radius-compat other

Related Commands show macfilter

config macfilter wlan-id

To modify a wireless LAN ID for a MAC filter, use the **config macfilter wlan-id** command.

config macfilter wlan-id *MAC wlan_id*

Syntax Description	config	Configure parameters.
	macfilter	Local MAC address filter
	wlan-id	Modify client wireless LAN ID.
	<i>MAC</i>	Client MAC address
	<i>wlan_id</i>	Wireless LAN Identifier to associate with. A value of zero is not allowed.

Defaults	None.

Examples	> config macfilter wlanid 11:11:11:11:11:11 2

Related Commands	show macfilter show wlan

Configure Management-User Commands

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

config mgmtuser add

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

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

Syntax Description	config	Configure parameters.
	mgmtuser	Management user account.
	add	Add a management user account.
	username	Account username. Up to 24 alphanumeric characters.
	password	Account password. Up to 24 alphanumeric characters.
	lobby-admin	Adds a management user of type lobby ambassodar who can create guest accounts.
	{read-write read-only}	- Enter read-write to create a management user with read-write access. - Enter read-only to create a management user with read-only access.
	[description]	Optional description of the account. Up to 32 alphanumeric characters within double quotes.

Defaults None.

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

Related Commands show mgmtuser

config mgmtuser delete

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

config mgmtuser delete *username*

Syntax Description

config	Configure parameters.
mgmtuser	Management user account.
delete	Delete a management user account.
<i>username</i>	Account username up to 24 alphanumeric characters.

Defaults

None.

Examples

```
> config mgmtuser delete admin
```

Deleted user admin

Related Commands

show mgmtuser

config mgmtuser description

To add a description to an existing management user login to the Cisco Wireless LAN controller, use the **config mgmtuser description** command.

config mgmtuser description *username description*

Syntax Description

config	Configure parameters.
mgmtuser	Management user account.
description	Add a description of the management user account.
<i>username</i>	Account username. Up to 24 alphanumeric characters.
<i>description</i>	Description of the account. Up to 32 alphanumeric characters within double quotes.

Defaults

None.

Examples

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

Related Commands

config mgmtuser add
config mgmtuser delete
config mgmtuser password
show mgmtuser

config mgmtuser password

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

config mgmtuser password *username password*

Syntax Description		
config		Configure parameters.
mgmtuser		Management user account
password		Add a management user account
<i>username</i>		Account username. Up to 24 alphanumeric characters.
<i>password</i>		Account password. Up to 24 alphanumeric characters.

Defaults None.

Examples > **config mgmtuser password admin 5rTfm**

Related Commands show mgmtuser

Configure Mobility Commands

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

config mobility group anchor

To configure the mobility wireless LAN anchor list, use the **config mobility group anchor** command.

```
config mobility group anchor {add | delete} wlan_id IP_address

config mobility group anchor {add | delete} guest_lan_id IP_address
```

Syntax Description	config	Configure parameters.
	mobility group	Mobility group member.
	{add delete}	- Enter add to add or change a mobility anchor to a wireless LAN. - Enter delete to delete a mobility anchor from a wireless LAN.
	wlan_id	Wireless LAN identifier between 1 and 16.
	guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).
	IP_address	Member switch IP address to anchor wireless LAN.

Defaults None.

```
Examples
> config mobility group anchor add 2 192.12.1.5
> config mobility group anchor delete 5 193.13.1.5
```

Related Commands

config mobility group domain

onfig mobility group member

config mobility group anchor add {wlan | guest-lan}

To create a new mobility anchor for the WLAN or wired guest LAN, use the **config mobility group anchor add {wlan | guest-lan}** command.

```
config mobility group anchor add {wlan | guest-lan} {wlan_id | guest_lan_id}
    anchor_controller_ip_address
```



Note You can also use the **config {wlan | guest-lan} mobility anchor add {wlan_id | guest_lan_id} anchor_controller_ip_address** command.



Note The *wlan_id* or *guest_lan_id* must exist and be disabled, and the *anchor_controller_ip_address* must be a member of the default mobility group.



Note Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor.

Syntax Description

config	Configure parameters.
mobility group	Mobility group member.
wlan	Wireless LAN parameters.
guest-lan	Indicates the active wired guest LAN.
add	Add a wireless LAN or a wired guest LAN.
<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 16.
<i>guest_lan_id</i>	Guest LAN indentifier between 1 and 5 (inclusive).
<i>anchor_controller_ip_a ddress</i>	IP address of the anchor controller.

Defaults

None.

Examples

```
> config mobility group anchor add {wlan|guest-lan} 5 255.255.255.0
```

Related Commands

```
config {wlan | guest-lan} mobility anchor add
config mobility group keepalive count
config mobility group keepalive interval
config mobility group anchor delete {wlan | guest-lan}
config {wlan | guest-lan} mobility anchor delete
```

config mobility group anchor delete {wlan | guest-lan}

To delete a new mobility anchor for the WLAN or wired guest LAN, use the **config mobility group anchor delete {wlan | guest-lan}** command.

```
config mobility group anchor delete {wlan | guest-lan} {wlan_id | guest_lan_id}
anchor_controller_ip_address
```



Note You can also use the **config {wlan | guest-lan} mobility anchor delete {wlan_id | guest_lan_id} anchor_controller_ip_address** command.



Note The *wlan_id* or *guest_lan_id* must exist and be disabled.



Note Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.

Syntax Description

config	Configure parameters.
mobility group	Mobility group member.
wlan	Wireless LAN parameters.
guest-lan	Indicates the active wired guest LAN.
delete	delete a wireless LAN or a wired guest LAN.
<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 16.
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
<i>anchor_controller_ip_address</i>	IP address of the anchor controller.

Defaults

None.

Examples

```
> config mobility group anchor delete {wlan|guest-lan} 5 255.255.255.0
```

Related Commands

```
config mobility group anchor add {wlan | guest-lan}
config mobility group keepalive count
config mobility group keepalive interval
config mobility group anchor delete {wlan | guest-lan}
config {wlan | guest-lan} mobility anchor delete
```


config mobility group domain

To configure the mobility domain name, use the **config mobility group domain** command.

config mobility group domain *domain_name*

Syntax Description	config	Configure parameters.
	mobility group	Mobility group member.
	domain	Enable or disable mobility group feature.
	<i>domain_name</i>	Domain name. Up to 31 characters; case sensitive.

Defaults	None.

Examples	> config mobility group domain lab1

Related Commands	show mobility summary config mobility group anchor config mobility group member

config mobility group keepalive count

To configure the controller to detect failed mobility group members (including anchor controllers), use the **config mobility group keepalive count** commands.

config mobility group keepalive count *count*—Specifies the number of times a ping request is sent to a mobility group member before the member is considered unreachable. The valid range is 3 to 20, and the default value is 3.

Syntax Description	config	Configure parameters.
	mobility group	Mobility group member.
	keepalive count	Specifies the number of times a ping request is sent to a mobility group member before the member is considered unreachable.
	<i>count</i>	The valide range is 3 to 20. The default is 3.

Defaults 3.

Examples > config mobility group keepalive count 3

Related Commands config mobility group keepalive interval

config mobility group keepalive interval

To configure the controller to detect failed mobility group members (including anchor controllers), use the **config mobility group keepalive** commands.

config mobility group keepalive interval *seconds*—Specifies the amount of time (in seconds) between each ping request sent to a mobility group member. The valid range is 1 to 30 seconds, and the default value is 10 seconds.

Syntax Description	config	Configure parameters.
	mobility group	Mobility group member.
	keepalive interval	Specifies the amount of time (in seconds) between each ping request sent to a mobility group member.
	<i>interval</i>	The valid range is 1 to 30 seconds. The default value is 10 seconds.

Defaults	config mobility group keepalive interval —10 seconds.

Examples	> config mobility group keepalive interval 10

Related Commands	config mobility group keepalive count

config mobility group member

To add or delete users from the mobility group member list, use the **config mobility group member** command.

```
config mobility group member {add MAC IP_address [group_name] | delete MAC}
```

Syntax Description	config	Configure parameters.
	mobility group member	Mobility group member.
	{add delete}	- Enter add to add or change a mobility group member to the list. - Enter delete to delete a mobility group member from the list.
	MAC	Member switch MAC address.
	IP_address	Member switch IP address.
	group_name	Optional member switch group name (if different from the default group name).

Defaults

None.

Examples

> config mobility group member add 11:11:11:11:11:11 192.12.1.2

Related Commands

show mobility summary

config mobility group anchor

config mobility group domain

config mobility group multicast-address

You can configure the multicast group IP address for non-local groups within the mobility list. To do so, enter this command:

```
config mobility group multicast-address group_name IP_address
```

Syntax Description	config	Configure parameters.
	mobility group	Mobility group
	multicast-address	Multicast address
	<i>group_name</i>	Optional member switch group name (if different from the default group name).
	<i>IP_address</i>	Member switch IP address.

Defaults	None.

Examples	> config mobility group multicast-address test 10.10.10.1

Related Commands	show mobility summary config mobility group anchor config mobility group domain

config mobility multicast-mode

To enable or disable multicast mobility mode, enter this command:

```
config mobility multicast-mode {enable | disable} local_group_multicast_address
```

Syntax Description	config	Configure parameters.
	mobility	Mobility multicast mode.
	multicast-mode	
	{enable disable}	- Enter enable to enable multicast mode, the controller uses multicast mode to send Mobile Announce messages to the local group - Enter disable to disable multicast mode, the controller uses unicast mode to send the Mobile Announce messages to the local group.
	local_group_multicast_address	IP address for the local mobility group

Defaults Disabled.

Examples > config mobility multicast-mode enable 157.168.20.0

Related Commands

show mobility summary

config mobility group multicast-address group_name IP_address

debug mobility multicast {enable | disable}

config mobility secure-mode

To configure the secure mode for mobility messages between Cisco Wireless LAN controllers, use the **config mobility secure-mode** command.

```
config mobility secure-mode {enable | disable}
```

Syntax Description	config	Configure parameters.
	mobility	Mobility group member.
	secure-mode	Configure the secure mode for mobility messages.
	{enable disable}	Enable or disable mobility group message security.

Defaults	None.

Examples	> config mobility secure-mode enable

Related Commands	show mobility summary

config mobility statistics reset

To reset the mobility statistics, use the **config mobility statistics** command.

config mobility statistics reset

Syntax Description

config	Configure parameters.
mobility	Mobility group.
statistics reset	Reset mobility group statistics.

Defaults

None.

Examples

```
> config mobility statistics reset
```

Related Commands

show mobility statistics

Configure Message Log Level Commands

Use the **config msglog** commands to configure msglog level settings.

config msglog level critical

To reset the message log so that it collects and displays only critical (highest-level) messages, use the **config msglog level critical** command.



Note

The message log always collects and displays critical messages, regardless of the message log level setting.

config msglog level critical

Syntax Description

config	Configure parameters.
msglog level	Configure msglog severity levels.
critical	Collect and display critical messages.

Defaults

Config msglog level error.

Examples

```
> config msglog level critical
```

```
> show msglog
```

```
Message Log Severity Level..... CRITICAL
(messages)
```

Related Commands

show msglog

config msglog level error

To reset the message log so that it collects and displays both critical (highest-level) and error (second-highest) messages, use the **config msglog level error** command.

config msglog level error

Syntax Description	config	Configure parameters.
	msglog level	Configure msglog severity levels.
	error	Collect and display critical and non-critical error messages.

Defaults Config msglog level error.

Examples

```
> config msglog level error

> show msglog

Message Log Severity Level..... ERROR
(messages)
```

Related Commands show msglog

config msglog level security

To reset the message log so that it collects and displays critical (highest-level), error (second-highest), and security (third-highest) messages, use the **config msglog level security** command.

config msglog level security

Syntax Description

config	Configure parameters.
msglog level	Configure msglog severity levels.
security	Collect and display critical, non-critical, and authentication- or security-related errors.

Defaults

Config msglog level error.

Examples

```
> config msglog level security

> show msglog

Message Log Severity Level..... SECURITY
(messages)
```

Related Commands

show msglog

config msglog level verbose

To reset the message log so that it collects and displays all messages, use the **config msglog level verbose** command.

config msglog level verbose

Syntax Description	config	Configure parameters.
	msglog level	Configure msglog severity levels.
	verbose	Collect and display all messages.

Defaults Config msglog level error.

Examples

```
> config msglog level verbose

> show msglog

Message Log Severity Level..... VERBOSE
(messages)
```

Related Commands show msglog

config msglog level warning

To reset the message log so that it collects and displays critical (highest-level), error (second-highest), security (third-highest), and warning (fourth-highest) messages, use the **config msglog level warning** command.

config msglog level warning

Syntax Description	config	Configure parameters.
	msglog level	Configure msglog severity levels.
	warning	Collect and display warning messages in addition to critical, non-critical, and authentication- or security-related errors.
Defaults	Config msglog level error.	
Examples	<pre>> config msglog level warning > show msglog Message Log Severity Level..... WARNING (messages)</pre>	
Related Commands	show msglog	

config nac acl

To configure the NAC ACL name for a Cisco Wireless LAN controller, use the **config nac acl** command.

```
config nac acl { none | acl-name }
```



Note

For a Cisco 2100 series wireless LAN controller, you must configure a pre-authentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any pre-authentication ACL for Cisco 4400 series wireless LAN controllers.

Syntax Description

config	Configure.
nac acl	Network Access Control acl.
{none acl-name}	- Enter none to clear the ACL name. - Enter <i>acl-name</i> to specify the ACL name.

Defaults

None.

Examples

```
> config nac acl none
```

Related Commands

show nac, config nac add, config nac delete, config nac disable, config nac enable, show nac summary, show nac statistics

config nac add

To add a NAC server index for a Cisco Wireless LAN controller, use the **config nac add** command.

config nac add *index IP_address port secret*

Syntax Description		
config		Configure.
nac		Network Access Control.
add		Command action.
<i>index</i>		NAC server index number.
<i>IP_address</i>		NAC server IP address.
<i>port</i>		NAC server UDP port number.
<i>secret</i>		NAC server secret.

Defaults None.

Examples > **config nac add none**

Related Commands

- show nac
- config nac acl
- config nac delete
- config nac disable
- config nac enable
- show nac summary
- show nac statistics

config nac delete

To delete a NAC server for a Cisco Wireless LAN controller, use the **config nac delete** command.

show nac delete *index*

Syntax Description

config	Configure.
nac	Network Access Control.
delete	Delete a NAC server.
<i>index</i>	NAC server index.

Defaults

None.

Examples

```
> config nac delete 23
```

Related Commands

show nac
config nac acl
config nac add
config nac disable
config nac enable
show nac summary
show nac statistics

config nac disable

To disable a NAC server for a Cisco Wireless LAN controller, use the **config nac disable** command.

show nac disable *index*

Syntax Description	config	Configure.
	nac	Network Access Control.
	disable	Disable a NAC server.
	<i>index</i>	Index number for NAC server.

Defaults	None.

Examples	> config nac disable 1

Related Commands	show nac config nac acl config nac add config nac delete show nac summary show nac statistics config nac enable

config nac enable

To enable a NAC server for a Cisco Wireless LAN controller, use the **config nac disable** command.

show nac enable *index*

Syntax Description	config	Configure.
	nac	Network Access Control.
	enable	Enable a NAC server.
	<i>index</i>	Index number for NAC server.

Defaults None.

Examples > **config nac disable 1**

Related Commands

- show nac
- config nac acl
- config nac add
- config nac delete
- show nac summary
- show nac statistics
- config nac disable

Configure Net User Commands

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

config netuser add

To add a guest user to the local network, use the **config netuser add** command.

To add a permanent user to the local user database on the controller—**config netuser add** *username password wlan wlan_id userType permanent description description*

To add a guest user on a WLAN or wired guest LAN to the local user database on the controller—**config netuser add** *username password { wlan_id | guestlan } { wlan_id | guest_lan_id } userType guest lifetime seconds description description*



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

Syntax	Description
<i>username</i>	Guest username. Up to 24 alphanumeric characters.
<i>password</i>	User password. Up to 24 alphanumeric characters.
<i>wlan_id</i>	Wireless LAN identifier assigned to the user. A zero value associates the user with any wireless LAN.
[<i>description</i>]	(Optional) Short description of user. Up to 32 characters enclosed in double-quotes.
guest	(Optional) Indicates a guest lifetime value is specified.
<i>lifetime_value</i>	Specify a lifetime value (60 to 259200 or 0) in seconds for the guest user.
Note A value of 0 indicates an unlimited lifetime.	

Defaults None.

Examples

This example adds a permanent user named Jane to the wireless network for 1 hour:

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

This example adds a guest user named George to the wireless network for 1 hour:

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

Related Commands

- show netuser
- config netuser delete

config netuser delete

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

config netuser delete *username*



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

Syntax Description

config	Configure parameters.
netuser	Local network user.
delete	Delete a user.
<i>username</i>	Network username. Up to 24 alphanumeric characters.

Defaults

None.

Examples

```
> config netuser delete able1
```

```
Deleted user able1
```

Related Commands

show netuser

config netuser description

To add a description to an existing net user, use the **config netuser description** command.

config netuser description *username description*

Syntax Description	config	Configure parameters.
	netuser	Local network user of up to 24 alphanumeric characters.
	description	Add a user description.
	<i>username</i>	Network username.
	<i>description</i>	Optional user description. Up to 32 alphanumeric characters enclosed in double quotes.

Defaults	None.

Examples	> config netuser description able1 "HQ1 Contact"

Related Commands	show netuser

config netuser guest-role apply

To apply a QoS role to a guest user, use the **config netuser guest-role apply** command.

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

 **Note** 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.

 **Note** 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.

Syntax Description

config	Configure parameters.
netuser	Local network user.
guest-role	QoS role for the guest user.
apply	Apply a QoS role to a guest user.
<i>username</i>	User name.
<i>role name</i>	QoS guest role name.

Defaults

None.

Examples

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

Related Commands

- config netuser guest-role create
- config netuser guest-role delete

config netuser guest-role create

To create a QoS role for a guest user, use the **config netuser guest-role create** command.

config netuser guest-role create *role_name*



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

Syntax Description

config	Configure parameters.
netuser	Local network user.
guest-role	QoS role for the guest user.
create	Create a user.
<i>role name</i>	QoS guest role name.

Defaults

None.

Examples

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

Related Commands

config netuser guest-role delete

config netuser guest-role delete

To delete a QoS role for a guest user, use the **config netuser guest-role delete** command.

config netuser guest-role delete *role_name*

Syntax Description

config	Configure parameters.
netuser	Local network user.
guest-role	QoS role for the guest user.
delete	Delete a user.
<i>role name</i>	QoS guest role name.

Defaults

None.

Examples

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

Related Commands

config netuser guest-role create

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

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

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



Note

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

Syntax Description

config	Configure parameters.
netuser	Local network user.
guest-role	QoS role for the guest user.
qos	Quality of service
data-rate	Rate in Kbps for TCP traffic.
average-data-rate	Average rate in Kbps for TCP traffic.
<i>role_name</i>	QoS guest role name.
<i>rate</i>	Rate for TCP traffic on a per user basis.

Defaults

None.

Examples

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

Related Commands

config netuser guest-role create

config netuser guest-role delete

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

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

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

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



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

Syntax Description

config	Configure parameters.
netuser	Local network user.
guest-role	QoS role for the guest user.
qos	Quality of service
data-rate	Rate in Kbps for TCP traffic.
average-realtime-rate	Average real-time rate for UDP traffic.
<i>role_name</i>	QoS guest role name.
<i>rate</i>	Rate for TCP traffic on a per user basis.

Defaults

None.

Examples

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

Related Commands

config netuser guest-role

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

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

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

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



Note 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.



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

Syntax Description

config	Configure parameters.
netuser	Local network user.
guest-role	QoS role for the guest user.
qos	Quality of service
data-rate	Rate in Kbps for TCP traffic.
burst-data-rate	Peak rate in Kbps for TCP traffic.
<i>role_name</i>	QoS guest role name.
<i>rate</i>	Rate for TCP traffic on a per user basis.

Defaults

None.

Examples

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

Related Commands

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

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

To configure the peak real-time data rate for UDP traffic on a per user basis, use the **config netuser guest-role qos data-rate burst-realtime-rate** command.

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



Note

The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.



Note

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

Syntax Description

config	Configure parameters.
netuser	Local network user.
guest-role	QoS role for the guest user.
qos	Quality of service
data-rate	Rate in Kbps for TCP traffic.
burst-realtime-rate	Peak real-time rate for UDP traffic.
<i>role_name</i>	QoS guest role name.
<i>rate</i>	Rate for TCP traffic on a per user basis.

Defaults

None.

Examples

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

Related Commands

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

config netuser maxEapUserLogin

To configure the maximum number of EAP user login attempts allowed for a network user, use the **config netuser maxEapUserLogin** command.

config netuser maxEapUserLogin *count*

Syntax Description	<i>count</i> Maximum number of login sessions for a single user. The allowed values are from 0 (unlimited) to 8.	
Defaults	0 (unlimited)	
Command History	Release	Modification
	4.1	This command was introduced.
Examples	<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* [**per method**]

Syntax Description

config	Configure parameters.
netuser	Local network user.
maxUserLogin	Configure the maximum number of login sessions allowed for a network user.
<i>count</i>	Maximum number of login sessions for a single user. The allowed values are from 0 (unlimited) to 8.

Defaults

0 (unlimited)

Examples

```
> config netuser maxuserlogin 8
```

Related Commands

show netuser

config netuser password

To change a local network user password, use the **config netuser password** command.

config netuser password *username password*

Syntax Description	config	Configure parameters.
	netuser	Local network user
	password	Modify the password.
	<i>username</i>	Network username. Up to 24 alphanumeric characters.
	<i>password</i>	Network user password. Up to 24 alphanumeric characters.

Defaults	None.

Examples	> config netuser password aire1 aire2

Related Commands	show netuser

config netuser wlan-id

To configure a wireless LAN ID for a network user, use the **config netuser wlan-id** command.

```
config netuser wlan-id username wlan_id
```

Syntax Description	config	Configure parameters.
	netuser	Local network user.
	wlan-id	Configure a wireless LAN ID for a network user.
	username	Network username. Up to 24 alphanumeric characters.
	wlan_id	Wireless LAN identifier to associate with the user. A zero value associates the user with any wireless LAN.

Defaults None.

Examples > config netuser wlan-id aire1 2

Related Commands show netuser
 show wlan summary

Configure Network Commands

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

config network 802.3-bridging

To enable or disable 802.3 bridging on a controller, use the **config network 802.3-bridging** command.

config network 802.3-bridging {enable | disable}

Syntax Description	enable	Enable 802.3 bridging.
	disable	Disable 802.3 bridging.

Defaults	Disabled.

Usage Guidelines	Because some applications use and relay 802.3 (LLC/SNAP) frame formats, you can enable the controller to support 802.3 bridging. When enabled, all 802.3 frames are forwarded to and from the client. The original LLC/SNAP and length of the frame is preserved during the encapsulation and decapsulation of the LWAPP data frame. For short frames, the trailer is stripped before the LWAPP header is added.

To determine the status of 802.3 bridging, enter the **show netuser guest-roles** command.

This command is only supported on the 2006 controller.

Examples	> config network 802.3-bridging enable

Related Commands	show netuser guest-roles

config network allow-old-bridge-aps

To configure an old bridge access point’s ability to associate with a switch, use the **config network allow-old-bridge-aps** command.

```
config network allow-old-bridge-aps {enable | disable}
```

Syntax Description	config	Configure parameters.
	network	Cisco Wireless LAN controller network parameter.
	allow-old-bridge-aps	Configure an old bridge access point’s ability to associate with a switch.
	{enable disable}	Enable or disable switch association.

Defaults Enabled.

Examples > config network allow-old-bridge-aps enable

Related Commands show network summary

config network ap-fallback

To configure Cisco lightweight access point fallback, use the **config network ap-fallback** command.

config network ap-fallback {enable | disable}

Syntax Description	config	Configure parameters.
	network	Cisco Wireless LAN controller network parameter.
	ap-fallback	Configure Cisco lightweight access point fallback.
	{enable disable}	Enable or disable Cisco lightweight access point fallback.

Defaults Enabled.

Examples > **config network ap-fallback enable**

Related Commands show network summary

config network ap-priority

To enable or disable the option to prioritize lightweight access points so that after a controller failure they reauthenticate by priority rather than on a first-come-until-full basis, use the **config network ap-priority** command.

config network ap-priority {enable | disable}

Syntax Description

config	Configure parameters.
network	Cisco Wireless LAN controller network parameter.
ap-priority	Configure lightweight access point priority reauthentication.
{enable disable}	Enable or disable lightweight access point priority reauthentication.

Defaults

Disabled.

Examples

```
> config network ap-priority enable
```

Related Commands

[config ap priority](#)
[show ap summary](#)
[show network summary](#)

config network apple-talk

To configure AppleTalk bridging, use the **config network apple-talk** command.

config network apple-talk { enable | disable }

Syntax Description	config	Configure parameters.
	network	Cisco Wireless LAN controller network parameter.
	apple-talk	Configure AppleTalk bridging.
	{ enable disable }	Enable or disable AppleTalk bridging.

Defaults None.

Examples > **config network apple-talk enable**

Related Commands show network summary

config network arptimeout

To set the ARP entry timeout value, use the **config network arptimeout** command.

config network arptimeout *seconds*

Syntax Description	config	Configure parameters.
	network	Cisco Wireless LAN controller network parameter.
	arptimeout	Set the ARP entry timeout value.
	<i>seconds</i>	Timeout in seconds. Minimum value is 10. Default value is 300.

Defaults	300

Examples	> config network arptimeout 240

Related Commands	show network summary

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command. This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.



Note

Zero-touch configuration must be enabled for this command to work.

config network bridging-shared-secret *shared_secret*

Syntax Description

config	Configure parameters.
network	Cisco Wireless LAN controller network parameter.
bridging-shared-secret	Configure the bridging shared secret.
<i>shared_secret</i>	Bridging shared secret string. Up to ten bytes.

Defaults

Enabled.

Examples

> **config network bridging-shared-secret shhh2**

Related Commands

show network summary

config network broadcast

To enable or disable broadcast packet forwarding, use the **config network broadcast** command. This command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. It uses the multicast mode configured on the controller (using the **config network multicast mode** command) to operate.

config network broadcast {enable | disable}

Syntax Description	config	Configure parameters.
	network	Network parameters.
	broadcast	Configure broadcast support.
	{enable disable}	Enable or disable broadcast packet forwarding.

Defaults	Disabled.

Examples	> config network broadcast enable

Related Commands	show network summary config network multicast global config network multicast mode

config network fast-ssid-change

To enable or disable fast SSID (Service Set Identifier) changing for mobile stations, use the **config network fast-ssid-change** command.

config network fast-ssid-change {enable | disable}

Syntax Description

config	Configure parameters.
network	Cisco Wireless LAN controller network parameter.
fast-ssid-change	Configure fast ssid on mobile stations.
{enable disable}	Enable or disable fast SSID changing for mobile stations.

Defaults

None.

Usage Guidelines

When you enable the Fast SSID Change feature, the controller allows clients to move between SSIDs. When the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID.

When you disable the FastSSID Change feature, the controller enforces a delay before clients are allowed to move to a new SSID.

Examples

```
> config network fast-ssid-change enable
```

Related Commands

show network summary

config network master-base

To enable or disable the Cisco Wireless LAN controller as an access point default master, use the **config network master-base** command. This setting is only used upon network installation and should be disabled after the initial network configuration.



Note

Because the Master Cisco Wireless LAN controller is normally not used in a deployed network, the Master Cisco Wireless LAN controller setting is automatically disabled upon reboot or OS code upgrade.

config network master-base {enable | disable}

Syntax Description	config	Configure parameters.
	network	Cisco Wireless LAN controller network parameter.
	master-base	Configure the Cisco Wireless LAN controller.
	{enable disable}	Enable or disable a Cisco Wireless LAN controller acting as a Cisco lightweight access point default master.

Defaults None.

Examples > **config network master-base enable**

Related Commands None.

config network mgmt-via-wireless

To enable Cisco Wireless LAN controller management from an associated wireless client, use the **config network mgmt-via-wireless** command.



Note

This feature allows wireless clients to manage only the Cisco Wireless LAN controller associated with the client AND the associated Cisco lightweight access point. That is, clients cannot manage another Cisco Wireless LAN controller with which they are not associated.

config network mgmt-via-wireless {enable | disable}

Syntax Description

config	Configure parameters.
network	Cisco Wireless LAN controller network parameter.
mgmt-via-wireless	Configure switch management via wireless interface.
{enable disable}	Enable or disable switch management via wireless interface.

Defaults

Disabled.

Examples

```
> config network mgmt-via-wireless enable
```

Related Commands

show network summary

config network multicast global

To enable or disable multicasting on the controller, use the **config network multicast global** command.

```
config network multicast global {enable | disable}
```

**Note**

The **config network broadcast {enable | disable}** command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. This command uses the multicast mode configured on the controller (using the **config network multicast mode** command) to operate.

Syntax Description	config	Configure parameters.
	network	Network parameters.
	multicast global	Configure multicast support.
	{enable disable}	Enable or disable multicast global support.

Defaults

Disabled.

Examples

> config network multicast global enable

Related Commands

show network summary
config network broadcast
config network multicast mode

config network multicast igmp snooping

To enable or disable IGMP snooping, use the **config network multicast igmp snooping** command.

config network multicast igmp snooping

Syntax Description	config	Configure parameters.
	network	Network parameters.
	multicast	Configure multicast support.
	igmp snooping	Internet Group Multicast Protocol snooping.

Defaults	None.

Examples	> config network multicast igmp snooping

Related Commands	config network multicast igmp timeout

config network multicast igmp timeout

To set the IGMP timeout value, use the **config network multicast igmp timeout** command.

config network multicast igmp timeout



Note

You can enter a timeout value between 30 and 300 seconds. The controller sends three queries in one timeout value at an interval of *timeout/3* to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

Syntax Description

config	Configure parameters.
network	Network parameters.
multicast	Configure multicast support.
igmp	Internet Group Multicast Protocol.
timeout	Number of seconds between 30 and 300.

Defaults

None.

Examples

```
> config network multicast igmp timeout
```

Related Commands

config network multicast igmp snooping

config network multicast mode multicast

To configure the controller to use the multicast method to send broadcast or multicast packets to an access point, use the **config network multicast mode multicast** command.

config network multicast mode multicast

Syntax Description

config	Configure parameters.
network	Network parameters.
multicast	Configure multicast support.
mode multicast	Sends a single copy of data to multiple receivers.

Defaults

None.

Examples

```
> config network multicast mode multicast
```

Related Commands

config network multicast global
config network broadcast
config network multicast mode unicast

config network multicast mode unicast

To configure the controller to use the unicast method to send broadcast or multicast packets to an access point, use the **config network multicast mode unicast** command.

config network multicast mode unicast

Syntax Description	config	Configure parameters.
	network	Network parameters.
	multicast	Configure multicast support.
	mode unicast	Sends multiple copies of data, one copy for each receiver.

Defaults None.

Examples > **config network multicast mode unicast**

Related Commands

config network multicast global

config network broadcast

config network multicast mode multicast

config network otap-mode

To enable or disable over-the-air provisioning (OTAP) of Cisco lightweight access points, use the **config network otap-mode** command.

config network otap-mode {enable | disable}

Syntax Description

config	Configure parameters.
network	Network parameters.
otap-mode	Configure OTAP provisioning.
{enable disable}	Enable or disable OTAP provisioning.

Defaults

Enabled.

Examples

```
> config network otap-mode disable
```

Related Commands

show network summary

config network rf-network-name

To set the RF-Network name, use the **config network rf-network-name** command.

config network rf-network-name *name*

Syntax Description	config	Configure parameters.
	network	Cisco Wireless LAN controller network parameter.
	rf-network-name	Set the RF-network name.
	<i>name</i>	RF-Network name. Up to 19 characters.

Defaults None.

Examples > **config network rf-network-name travelers**

Related Commands **show network summary**

config network secureweb

To change the state of the secure web (https = http + SSL) interface, use the **config network secureweb** command.

config network secureweb {enable | disable}



Note This command allows users to access the controller GUI using *http://ip-address*. Web mode is *not* a secure connection.

Syntax Description

config	Configure parameters.
network	Network parameters.
secureweb	Configure the secure web interface.
{enable disable}	Enable or disable the secure web interface.

Defaults

Enabled.

Examples

```
> config network secureweb enable
```

You must reboot for the change to take effect.

Related Commands

show network summary

config network secureweb cipher-option high

config network secureweb cipher-option high

To enable or disable secure web mode with increased security, use the **config network secureweb cipher-option high** command.

config network secureweb cipher-option high {enable | disable}



Note This command allows users to access the controller GUI using *http://ip-address* but only from browsers that support 128-bit (or larger) ciphers.

Syntax Description	config	Configure parameters.
	network	Network parameters.
	secureweb	Configure the secure web interface.
	{enable disable}	Enable or disable the secure web interface.

Defaults Disabled.

Examples > **config network secureweb cipher-option high enable**

Related Commands **show network summary**
config network secureweb

config network ssh

To allow or disallow new ssh sessions, use the **config network ssh** command.

config network ssh {enable | disable}

Syntax Description

config	Configure parameters.
network	Network parameters.
ssh	Secure Shell sessions
{enable disable}	Allow or disallow new ssh sessions.

Defaults

Enabled.

Examples

```
> config network ssh enable
```

Related Commands

show network summary

config network telnet

To allow or disallow new telnet sessions, use the **config network telnet** command.

config network telnet {enable | disable}

Syntax Description

config	Configure parameters.
network	Network parameters.
telnet	Configure new telnet sessions.
{enable disable}	Allow or disallow new telnet sessions.

Defaults

Disabled.

Examples

```
> config network telnet enable
```

Related Commands

show network summary

config network usertimeout

To change the timeout for idle client sessions, use the **config network usertimeout** command. Use this command to set the idle client session duration on the Cisco Wireless LAN controller. The minimum duration is 10 seconds.

config network usertimeout *seconds*

Syntax Description	
config	Configure parameters.
network	Network parameters.
usertimeout	Configure idle session timeout.
<i>seconds</i>	Timeout duration in seconds. Minimum value is 10. Default value is 300.

Defaults 300

Examples > **config network usertimeout 1200**

Related Commands show network summary

config network web-auth-port

To configure an additional port to be redirected for web authentication, use the **config network web-auth-port** command.

config network web-auth-port *port*

Syntax Description	config	Configure parameters.
	network	Network parameters.
	web-auth-port	Configure an additional port to be redirected for web authentication.
	<i>port</i>	Port number.

Defaults	None.

Examples	> config network web-auth-port 1200

Related Commands	show network summary

config network webmode

To enable or disable the web mode, use the **config network webmode** command.

config network webmode {enable | disable}

Syntax Description	config	Configure parameters.
	network	Network parameters.
	webmode	Configure web user interface access.
	{enable disable}	Enable or disable the web interface.

Defaults	Enabled.

Examples	> config network webmode disable

Related Commands	show network summary

config network zero-config

To configure bridge access point ZeroConfig support, use the **config network zero-config** command.

config network zero-config {enable | disable}

Syntax Description	config	Configure parameters.
	network	Cisco Wireless LAN controller network parameter.
	zero-config	Configure bridge access point ZeroConfig support.
	{enable disable}	Enable or disable bridge access point ZeroConfig support.

Defaults	Enabled.

Examples	> config network zero-config enable

Related Commands	show network summary

config nmosp notify-interval measurement



Note

The TCP port (16113) that the controller and location appliance communicate over must be open (not blocked) on any firewall that exists between the controller and the location appliance for Network Mobility Services Protocol (NMSP) to function.

To modify the NMSP notification interval value on the controller to address latency in the network, use the **config nmosp notify-interval measurement** command.

config nmosp notify-interval measurement {**client** | **rfid** | **rogue**} *interval*

Syntax Description

config	Configure parameters.
nmosp notify-interval measurement	Modify the NMSP notification interval.
client	Modify the interval for clients,
rfid	Modify the interval for active RFID tags.
rogue	Modify the interval for rogue access points and rogue clients.
<i>interval</i>	Between 1 and 30 seconds

Defaults

None

Examples

```
> config nmosp notify-interval measurement rfid 25
```

Related Commands

[show nmosp notify-interval summary](#)

config pmk-cache delete

To delete an entry in the PMK cache from all Cisco Wireless LAN controllers in the mobility group, use the **config pmk-cache delete** command.

config pmk-cache delete {all | MAC}

Syntax Description	config	Configure parameters.
	pmk-cache delete	Delete an entry in the PMK cache.
	{all MAC}	- Enter all to delete all Cisco Wireless LAN controllers. - Enter the MAC address of the Cisco Wireless LAN controller to delete.

Defaults	None.

Examples	> config pmk-cache delete all

Related Commands	show pmk-cache

Configure Port Commands

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

config port adminmode

To configure the administration mode of a single port or all Cisco Wireless LAN controller ports, use the **config port adminmode** command.

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

Syntax Description	config	Configure parameters.
	port	Port parameters.
	adminmode	Administrative mode.
	{ all <i>port</i> }	- Enter all to configure all ports. - Enter the number of the port to configure.
	{ enable disable }	Enable or disable the specified ports.

Defaults Enabled.

Examples

To disable port 8:

```
> config port adminmode 8 disable
```

To enable all ports:

```
> config port adminmode all enable
```

Related Commands show port

config port autoneg

To configure 10/100BASE-T Ethernet ports for physical port autonegotiation, use the **config port autoneg** command.



Note

Port autoconfiguration must be disabled before you make physical mode manual settings using the config port physicalmode command. Also note that the config port autoneg command overrides settings made using the config port physicalmode command.

config port autoneg {all | port} {enable | disable}

Syntax Description

config	Configure parameters.
port	10/100BASE-T Ethernet.
autoneg	Configure a port's auto negotiation mode.
{all port}	- Enter all to configure all ports. - Enter the number of the port to configure.
{enable disable}	Enable or disable the specified ports.

Defaults

All Ports = autonegotiation enabled.

Examples

To turn on physical port autonegotiation for all front-panel Ethernet ports:

> **config port autoneg all enable**

To disable physical port autonegotiation for front-panel Ethernet port 19:

> **config port autoneg 19 disable**

Related Commands

show port
config port physicalmode

config port linktrap

To change up/down trap settings for link status alert for a single port or all Cisco Wireless LAN controller ports, use the **config port linktrap** command.

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

Syntax Description	
config	Configure parameters.
port	Port parameters.
linktrap	Link status alert.
{all <i>port</i> }	- Enter all to configure all ports. - Enter the number of the port to configure.
{enable disable}	Enable or disable the specified ports.

Defaults Enabled.

Examples

To disable port 8 traps:

```
> config port linktrap 8 disable
```

To enable all port traps:

```
> config port linktrap all enable
```

Related Commands show port

config port multicast appliance

To change the multicast appliance service for a single port or all Cisco Wireless LAN controller ports, use the **config port multicast appliance** command.

```
config port multicast appliance port {enable | disable}
```

Syntax Description	config	Configure parameters.
	port	Port parameters.
	multicast appliance	Configure multicast appliance service for the specified port.
	port	Number of the port to configure.
	{enable disable}	Enable or disable service for the specified port.

Defaults	Enabled.

Examples	To enable appliance service for port 3: <pre>> config port multicast appliance 3 enable</pre>

Related Commands	show port

config port physicalmode

To set any or all front-panel 10/100BASE-T Ethernet ports for dedicated 10 Mbps or 100 Mbps, Half or Full Duplex operation, use the **config port physicalmode** command.

Note that you must disable autonegotiation using the **config port autoneg** command before manually configuring any port's physical mode. Also note that the **config port autoneg** command overrides settings made using the **config port physicalmode** command.

config port physicalmode {all | port} {100h | 100f | 10h | 10f}

Syntax Description		
config		Configure parameters.
port		Port parameters.
physicalmode		Port physical mode.
{all port}		- Enter all to configure all ports. - Enter the number of the port to configure.
{100h 100f 10h 10f}		- Enter 100h for 100 Mbps/Half Duplex operation. - Enter 100f for 100 Mbps/Full Duplex operation. - Enter 10h for 10 Mbps/Half Duplex operation. - Enter 10f for 10 Mbps/Full Duplex operation.

Defaults

All Ports are set to auto negotiate.

Examples

To set all ports to 100 Mbps/Full Duplex operation:

```
> config port physicalmode all 100f
```

To set port 20 to 100 Mbps/Half Duplex operation:

```
> config port physicalmode 20 100h
```

To set port 21 to 10 Mbps/Full Duplex operation:

```
> config port physicalmode 21 10f
```

To set port 22 to 10 Mbps/Half Duplex operation:

```
> config port physicalmode 22 10h
```

Related Commands

config port autoneg
show port

config port power

To configure a Cisco Wireless LAN controller’s port’s power over ethernet, use the **config port power** command.

```
config port power {all | port} {enable | disable}
```

Syntax Description	config	Configure parameters.
	port	Port parameters.
	power	Configure a port’s power over ethernet.
	{all port}	• Enter all to configure all ports. • Enter the number of the port to configure.
	{enable disable}	Enable or disable the specified ports.

Defaults	Enabled.

Examples	To enable all ports’ power: > config port power all enable

Related Commands	show port

config prompt

To change the CLI system prompt, use the **config prompt** command.

config prompt *prompt*

Because the system prompt is a user-defined variable, it is omitted from the rest of this documentation.

Syntax Description

config	Configure parameters.
prompt	Change the CLI system prompt.
<i>prompt</i>	New CLI system prompt enclosed in double quotes. Up to 31 alphanumeric characters; case sensitive.

Defaults

The system prompt is configured using the startup wizard.

Examples

```
> config prompt "Cisco 4400"  
(Cisco 4400)>
```

Related Commands

None.

config qos average-data-rate

To define the average data rate in Kbps for TCP traffic per user, use the **config qos average-data-rate** command.

```
config qos average-data-rate { bronze | silver | gold | platinum } rate
```

**Note**

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 profile.

Syntax Description	config qos	Command action.
	average-data-rate	Rate in Kbps for TCP traffic.
	{bronze silver gold platinum}	Enter one of the four supported queue names.

Defaults

None.

Examples

> config qos average-data-rate gold 0

Related Commands

show qos description

config qos burst-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config qos max-rf-usage

config qos average-realtime-rate

To define the average real-time data rate in Kbps for UDP traffic per user, use the **config qos average-realtime-rate** command.

```
config qos average-realtime-rate {bronze | silver | gold | platinum} rate
```

Syntax Description

config qos	Command action.
average-realtime-rate	Average actual rate in Kbps for UDP traffic.
{bronze silver gold platinum}	Enter one of the four supported queue names.

Defaults

None.

Examples

```
> config qos average-realtime-rate gold rate
```

Related Commands

show qos description
config qos average-data-rate
config qos burst-data-rate
config qos burst-realtime-rate
config qos max-rf-usage

config qos burst-data-rate

To define the peak data rate in Kbps for TCP traffic per user, use the **config qos burst-data-rate** command.

```
config qos burst-data-rate { bronze | silver | gold | platinum } rate
```

Syntax Description	config qos	Command action.
	burst-data-rate	Peak rate in Kbps for TCP traffic.
	{bronze silver gold platinum}	Enter one of the four supported queue names.

Defaults	None.

Examples	> config qos burst-data-rate gold 30000

Related Commands	show qos description, onfig qos average-data-rate config qos average-realtime-rate config qos burst-realtime-rate config qos max-rf-usage

config qos burst-realtime-rate

To define the average real-time data rate in Kbps for UDP traffic per user, use the **config qos burst-realtime-rate** command.

```
config qos burst-realtime-rate {bronze | silver | gold | platinum} rate
```

Syntax Description	config qos	Command action.
	burst-realtime-rate	Peak actual rate in Kbps for UDP traffic.
	{bronze silver gold platinum}	Enter one of the four supported queue names.

Defaults	None.

Examples	> config qos burst-realtime-rate gold rate

Related Commands	show qos description
	config qos average-data-rate
	config qos burst-data-rate
	config qos average-realtime-rate
	config qos max-rf-usage

config qos description

To change the profile description, use the **config qos description** command.

```
config qos description { bronze | silver | gold | platinum } description
```

Syntax Description	config qos	Command action.
	description	Configure QoS profile description.
	{bronze silver gold platinum}	Enter one of the four supported queue names.

Defaults	None.

Examples	> config qos description gold <i>description</i>

Related Commands	show qos average-data-rate config qos burst-data-rate config qos average-realtime-rate config qos burst-realtime-rate config qos max-rf-usage

config qos max-rf-usage

To specify the maximum percentage of RF usage per access point, use the **config qos max-rf-usage** command.

```
config qos max-rf-usage { bronze | silver | gold | platinum } usage_percentage
```

Syntax Description	config qos	Command action.
	max-rf-usage	Maximum percentage of RF usage.
	{bronze silver gold platinum}	Enter one of the four supported queue names.

Defaults	None.

Examples	> config qos max-rf-usage gold 20

Related Commands	show qos description
	config qos average-data-rate
	config qos burst-data-rate
	config qos average-realtime-rate
	config qos burst-realtime-rate

config qos protocol-type/config qos dot1p-tag

To define the maximum value (0-7) for the priority tag associated with packets that fall within the profile, use the **config qos protocol-type** and **config qos dot1p-tag** commands.

```
config qos protocol-type {bronze | silver | gold | platinum} {none | dot1p}

config qos dot1p-tag {bronze | silver | gold | platinum} dot1p_tag
```

Syntax Description

config qos	Command action.
protocol-type	Configure the QoS protocol type (bronze, silver, gold, platinum)
dot1p-tag	Configure a QoS 802.1p tag.
{bronze silver gold platinum}	Enter one of the four supported queue names.
none	Enter when no specific protocol is assigned.
dot1p	Specify a 802.1p tag.
dot1p_tag	Specify a dot1p tag value of between 1 and 7.

Defaults

None.

Examples

```
> config qos protocol-type silver dot1p
> config qos dot1p-tag gold 5
```

Related Commands

show qos queue_length all

config qos queue_length

To specify the maximum number of packets that access points keep in their queues, use the **config qos queue_length** command.

```
config qos queue_length { bronze | silver | gold | platinum } queue_length
```

Syntax Description	config qos	Command action.
	queue_length	Configure QoS queue length.
	{bronze silver gold platinum}	Enter one of the four supported queue names.
	<i>length</i>	Enter the maximum queue length value (10 to 255).

Defaults	None.

Examples	> config qos queue_length gold 12

Related Commands	show qos [bronze silver gold platinum]

Configure Radius Account Commands

Use the **config radius acct** commands to configure RADIUS account server settings.

config radius acct add

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

```
config radius acct add index ip_address port {ascii | hex} secret
```

Syntax Description

config	Configure parameters.
radius acct	RADIUS accounting server.
add	Add a RADIUS server.
<i>index</i>	RADIUS server index. Cisco Wireless LAN controller begins search with 1.
<i>ip_address</i>	RADIUS server's IP address.
<i>port</i>	RADIUS server's UDP port number for the interface protocols.
{ascii hex}	RADIUS server's secret type: ascii or hex .
<i>secret</i>	RADIUS server's secret.

Defaults

When added the port number defaults to 1813 and state is enabled.

Examples

To configure a priority 1 RADIUS 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 delete

To delete a RADIUS accounting server for the Cisco Wireless LAN controller, use the **config radius acct delete** command.

config radius acct delete *index*

Syntax Description

config	Configure parameters.
radius acct	RADIUS accounting server.
delete	Delete a RADIUS server.
<i>index</i>	RADIUS server index.

Defaults

None.

Examples

```
> config radius acct delete 1
```

Related Commands

show radius acct statistics

config radius acct disable

To disable a RADIUS accounting server for the Cisco Wireless LAN controller, use the **config radius acct disable** command.

config radius acct disable *index*

Syntax Description	config	Configure parameters.
	radius acct	RADIUS accounting server.
	disable	Disable a RADIUS server.
	<i>index</i>	RADIUS server index.

Defaults	None.

Examples	> config radius acct disable 1

Related Commands	show radius acct statistics

config radius acct enable

To enable a RADIUS accounting server for the Cisco Wireless LAN controller, use the **config radius acct enable** command.

config radius acct enable *index*

Syntax Description

config	Configure parameters.
radius acct	RADIUS accounting server.
enable	Enable a RADIUS server.
<i>index</i>	RADIUS server index.

Defaults

None.

Examples

```
> config radius acct enable 1
```

Related Commands

show radius acct statistics

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

config	Configure parameters.
radius	RADIUS accounting server.
fallback-test	Configure the RADIUS server fallback behavior.
mode {off passive active}	• Off disables RADIUS server fallback. • Passive causes the controller to revert to a preferable server (with a lower server index) from the available backup servers without using extraneous probe messages. The controller simply ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent. • Active causes the controller to revert to a preferable server (with a lower server index) from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller simply ignores all inactive servers for all active RADIUS requests.
username	Specifies the name to be sent in the inactive server probes.
<i>username</i>	You can enter up to 16 alphanumeric characters for the <i>username</i> parameter.
interval	Specifies the probe interval value.
<i>interval</i>	Probe interval range is 180 to 3600.

Defaults

Default probe interval: 300.

Examples

```
> config radius fallback-test mode off
> config radius fallback-test mode passive
> config radius fallback-test mode active
> config radius fallback-test username user_1
> config radius fallback-test interval 500
```

Related Commands

show radius acct statistics

config radius acct network

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

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

Syntax Description	config	Configure parameters.
	radius acct	Default RADIUS accounting server.
	network	Configure a default RADIUS server for network users.
	<i>index</i>	RADIUS server index.
	{ enable disable }	Enable or disable the server as a network user's default RADIUS Server.

Defaults	None.

Examples	> config radius acct network 1 enable

Related Commands	show radius acct statistics

config radius acct ipsec authentication

To configure IPSec authentication for the Cisco Wireless LAN controller, use the **config radius acct ipsec authentication** command.

```
config radius acct ipsec authentication { hmac-md5 | hmac-sha1 } index
```

Syntax Description	config	Configure parameters.
	radius acct	RADIUS accounting server.
	ipsec authentication	Configure IPSec authentication service.
	{hmac-md5 hmac-sha1}	- Enter hmac-md5 to enable IPSec HMAC-MD5 authentication. - Enter hmac-sha1 to IPSec HMAC-SHA1 authentication.
	index	RADIUS server index.

Defaults None.

Examples > config radius acct ipsec authentication hmac-md5 1

Related Commands show radius acct statistics

config radius acct ipsec disable

To disable IPSec support for an accounting server for the Cisco Wireless LAN controller, use the **config radius acct ipsec disable** command.

config radius acct ipsec disable *index*

Syntax Description

config	Configure parameters.
radius acct	RADIUS accounting server.
ipsec disable	Disable IPSec support for an accounting server.
<i>index</i>	RADIUS server index.

Defaults

None.

Examples

```
> config radius acct ipsec disable 1
```

Related Commands

show radius acct statistics

config radius acct ipsec enable

To enable IPSec support for an accounting server for the Cisco Wireless LAN controller, use the **config radius acct ipsec enable** command.

config radius acct ipsec enable *index*

Syntax Description	config	Configure parameters.
	radius acct	RADIUS accounting server.
	ipsec enable	Enable IPSec support for an accounting server.
	<i>index</i>	RADIUS server index.

Defaults	None.

Examples	> config radius acct ipsec enable 1

Related Commands	show radius acct statistics

config radius acct ipsec encryption

To configure IPSec encryption for an accounting server for the Cisco Wireless LAN controller, use the **config radius acct ipsec encryption** command.

config radius acct ipsec encryption {3des | aes | des} index

Syntax Description	
config	Configure parameters.
radius acct	RADIUS accounting server.
ipsec encryption	Configure IPSec encryption.
{3des aes des}	- Enter 3des to enable IPSec 3DES Encryption. - Enter aes to enable IPSec AES Encryption. - Enter des to enable IPSec DES Encryption.
index	Enter a RADIUS server index value of between 1 and 17.

Defaults None.

Examples > **config radius acct ipsec encryption 3des 3**

Related Commands

- show radius acct statistics
- show radius summary

config radius acct ipsec ike

To configure Internet Key Exchange (IKE) for the Cisco Wireless LAN controller, use the **config radius acct ipsec** command.

```
config radius acct ipsec ike {dh-group {group-1 | group-2 | group-5} |
    lifetime seconds | phase1 {aggressive | main}} index
```

Syntax Description	
config	Configure parameters.
radius acct	RADIUS accounting server.
ipsec ike	Configure IKE.
dh-group {group-1 group-2 group-5}	Configure the IKE Diffie-Hellman group. - Enter group-1 to configure DH Group 1 (768 bits). - Enter group-2 to configure DH Group 2 (1024 bits). - Enter group-5 to configure DH Group 2 (1024 bits).
lifetime seconds	Configure the IKE lifetime in seconds.
phase1 {aggressive main}	Configure the IKE Phase1 mode. - Enter aggressive to enable the aggressive mode. - Enter main to enable the main mode.
index	RADIUS server index.

Defaults None.

Examples > config radius acct ipsec ike lifetime 23 1

Related Commands show radius acct statistics

config radius acct retransmit-timeout

To change the default transmission timeout for a RADIUS accounting server for the Cisco Wireless LAN controller, use the **config radius acct retransmit-timeout** command.

config radius acct retransmit-timeout *index timeout*

Syntax Description		
config		Configure parameters.
radius acct		RADIUS accounting server.
retransmit-timeout		Configure retransmission timeout.
<i>index</i>		RADIUS server index.
<i>timeout</i>		Number of seconds (from 2 to 30) between retransmissions.

Defaults	None.

Examples	> config radius acct retransmit-timeout 5

Related Commands	show radius acct statistics

Configure RADIUS Authentication Server Commands

Use the **config radius auth** commands to configure RADIUS authentication server settings.

config radius auth add

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

```
config radius auth add index ip_address port {ascii | hex} secret
```

Syntax Description	config	Configure parameters.
	radius auth	RADIUS authentication server.
	add	Add a RADIUS server.
	<i>index</i>	RADIUS server index. Cisco Wireless LAN controller begins search with 1.
	<i>ip_address</i>	RADIUS server's IP address.
	<i>port</i>	RADIUS server's UDP port number for the interface protocols.
	{ascii hex}	RADIUS server's secret type: ascii or hex .
	<i>secret</i>	RADIUS server's secret.

Defaults

When added the port number defaults to 1812 and state is enabled.

Examples

To configure a priority 1 RADIUS 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 delete

To delete a RADIUS authentication server for the Cisco Wireless LAN controller, use the **config radius auth delete** command.

config radius auth delete *index*

Syntax Description

config	Configure parameters.
radius auth	RADIUS authentication server.
delete	Delete a RADIUS server.
<i>index</i>	RADIUS server index.

Defaults

None.

Examples

```
> config radius auth delete 1
```

Related Commands

show radius auth statistics

config radius auth disable

To disable a RADIUS authentication server for the Cisco Wireless LAN controller, use the **config radius auth disable** command.

config radius auth disable *index*

Syntax Description	config	Configure parameters.
	radius auth	RADIUS authentication server.
	disable	Disable a RADIUS server.
	<i>index</i>	RADIUS server index.

Defaults	None.

Examples	> config radius auth disable 1

Related Commands	show radius auth statistics

config radius auth enable

To enable a RADIUS authentication server for the Cisco Wireless LAN controller, use the **config radius auth enable** command.

config radius auth enable *index*

Syntax Description

config	Configure parameters.
radius auth	RADIUS authentication server.
enable	Enable a RADIUS server.
<i>index</i>	RADIUS server index.

Defaults

None.

Examples

```
> config radius auth enable 1
```

Related Commands

show radius auth statistics

config radius auth ipsec authentication

To configure IPSec support for an authentication server for the Cisco Wireless LAN controller, use the **config radius auth ipsec authentication** command.

config radius auth ipsec authentication {hmac-md5 | hmac-sha1} index

Syntax Description	config	Configure parameters.
	radius auth	RADIUS authentication server.
	ipsec authentication	Configure IPSec authentication service.
	{hmac-md5 hmac-sha1}	- Enter hmac-md5 to enable IPSec HMAC-MD5 authentication. - Enter hmac-sha1 to IPSec HMAC-SHA1 authentication.
	index	RADIUS server index.

Defaults None.

Examples > config radius auth ipsec authentication hmac-md5 1

Related Commands show radius acct statistics

config radius auth ipsec disable

To disable IPSec support for an authentication server for the Cisco Wireless LAN controller, use the **config radius auth ipsec disable** command.

config radius auth ipsec {enable | disable} index

Syntax Description	config	Configure parameters.
	radius auth	RADIUS authentication server.
	ipsec {enable disable}	- Enter enable to enable IPSec support for an authentication server. - Enter disable to disable IPSec support for an authentication server.
	index	RADIUS server index.

Defaults	None.

Examples	<pre>> config radius auth ipsec enable 1 > config radius auth ipsec disable 1</pre>

Related Commands	show radius acct statistics

config radius auth ipsec encryption

To configure IPSec support for an authentication server for the Cisco Wireless LAN controller, use the **config radius auth ipsec** command.

```
config radius auth ipsec encryption {3des | aes | des} index
```

Syntax Description	config	Configure parameters.
	radius auth	RADIUS authentication server.
	ipsec encryption	Configure IPSec encryption.
	{3des aes des}	- Enter 3des to enable IPSec 3DES Encryption. - Enter aes to enable IPSec AES Encryption. - Enter des to enable IPSec DES Encryption.
	index	RADIUS server index.

Defaults None.

Examples > config radius acct ipsec encryption 3des 3

Related Commands show radius acct statistics

config radius auth ipsec ike

To configure IKE for the Cisco Wireless LAN controller, use the **config radius auth ipsec ike** command.

```
config radius auth ipsec ike {dh-group {group-1 | group-2 | group-5} |  
lifetime seconds | phase1 {aggressive | main}} index
```

Syntax	Description
config	Configure parameters.
radius auth	RADIUS authentication server.
ipsec ike	Configure IKE.
dh-group {group-1 group-2 group-5}	Configure the IKE Diffie-Hellman group. - Enter group-1 to configure DH Group 1 (768 bits). - Enter group-2 to configure DH Group 2 (1024 bits). - Enter group-5 to configure DH Group 2 (1024 bits).
lifetime seconds	Configure the IKE lifetime in seconds.
phase1 {aggressive main}	Configure the IKE Phase1 mode. - Enter aggressive to enable the aggressive mode. - Enter main to enable the main mode.
index	RADIUS server index.

Defaults None.

Examples

```
> config radius auth ipsec ike lifetime 23 1
```

Related Commands show radius acct statistics

config radius auth keywrap

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

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

Syntax Description

config	Configure parameters.
radius auth	RADIUS authentication server.
keywrap	Configure AES key wrap
{enable disable add}	- Enter enable to enable AES key wrap. - Enter disable to disable AES key wrap. - Enter add to configure the AES key wrap attributes.
{ascii hex}	- Enter ascii to configure the key wrap in ascii format. - Enter hex to configure the key wrap in hexadecimal format.
kek	Specifies the 16-byte Key Encryption Key (KEK).
mack	Specifies the 20-byte Message Authentication Code Key (MACK).
index	Specifies the index of the RADIUS authentication server on which to configure the AES key wrap.

Defaults

None.

Examples

```
> config radius auth keywrap enable
> config radius auth keywrap disable
> config radius auth keywrap add ascii kek mack index
```

Related Commands

show radius auth statistics

config radius auth management

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

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

Syntax Description	config	Configure parameters.
	radius auth	Default RADIUS authentication server.
	management	Configure a RADIUS server for management users.
	index	RADIUS server index.
	{enable disable}	Enable or disable the server as a management user’s default RADIUS Server.

Defaults None.

Examples > config radius auth management 1 enable

Related Commands show radius acct statistics
config radius acct network

config radius auth network

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

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

Syntax Description	config	Configure parameters.
	radius auth	Default RADIUS authentication server.
	network	Configure a default RADIUS server for network users.
	<i>index</i>	RADIUS server index.
	{enable disable}	Enable or disable the server as a network user default RADIUS Server.

Defaults	None.

Examples	> config radius auth network 1 enable

Related Commands	show radius acct statistics config radius acct network

config radius auth retransmit-timeout

To change the default transmission timeout for a RADIUS authentication server for the Cisco Wireless LAN controller, use the **config radius auth retransmit-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description	config	Configure parameters.
	radius auth	RADIUS authentication server.
	retransmit-timeout	Configure retransmission timeout.
	<i>index</i>	RADIUS server index.
	<i>timeout</i>	Number of seconds (from 2 to 30) between retransmissions.

Defaults	None.

Examples	> config radius auth retransmit-timeout 5

Related Commands	show radius auth statistics

config radius auth rfc3576

To configure RADIUS rfc3576 support for the authentication server for the Cisco Wireless LAN controller, use the **config radius auth rfc3576** command.

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

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

Syntax Description	config	Configure parameters.
	radius auth	Default RADIUS authentication server.
	rfc3576	Configure RADIUS rfc3576 support.
	{enable disable}	Enable or disable RFC-3576 support for an authentication server.
	<i>index</i>	RADIUS server index.

Defaults	None.

Examples	> config radius auth rfc3576 enable 2

Related Commands	show radius auth statistics show radius summary show radius rfc3576

config radius auth server-timeout

To configure the retransmission timeout value for a RADIUS accounting server, use the **config radius auth server-timeout** command.

config radius auth server-timeout *index timeout*

Syntax Description	config	Configure parameters.
	radius auth	Default RADIUS authentication server.
	server-timeout	Configure the retransmission timeout value for a RADIUS accounting server
	<i>index</i>	RADIUS server index.
	<i>timeout</i>	Timeout value, valid range is 2 to 30 seconds

Defaults Default timeout: 2 seconds.

Examples > **config radius auth server-timeout 2 10**

Related Commands show radius auth statistics
show radius summary

config radius aggressive-failover disabled

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

config radius aggressive-failover disabled

Syntax Description

This command does not have any arguments or keywords.

Defaults

This command has no defaults.

Command History

Release	Modification
3.2.171	This command was introduced.

Examples

> **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** command.

config radius backward compatibility {enable | disable}

Syntax Description	config	Configure parameters.
	radius backward	RADIUS authentication server.
	compatibility	Configure RADIUS backward compatibility.
	{enable disable}	Enable or disable RADIUS vendor ID backward compatibility.

Defaults Enabled.

Examples > **config radius backward compatibility disable**

Related Commands show radius summary

config radius callStationIdType

To configure callStationIdType information sent in radius messages for the Cisco Wireless LAN controller, use the **config radius callStationIdType** command. This command uses the selected calling station ID for communications with RADIUS servers and other applications.

```
config radius callStationIdType {ipAddr | macAddr | ap-macAddr}
```

Syntax Description	config	Configure parameters.
	radius	Configure callStationIdType information.
	callStationIdType	
	{ipAddr macAddr ap-macAddr}	- Enter ipAddr to configure Call Station ID type to IP address (only layer 3). - Enter macAddr to configure Call Station ID type to the system’s MAC address (layers 2 and 3). - Enter ap-macAddr to configure Call Station ID type to use the access point’s MAC address (layers 2 and 3).

Defaults Enabled.

Examples

```
> config radius callStationIdType ipAddr
> config radius callStationIdType macAddr
> config radius callStationIdType ap-macAddr
```

Related Commands show radius summary

config rfid auto-timeout

To configure the automatic timeout of RFID tags, use the **config rfid auto-timeout** command.

config rfid auto-timeout {enable | disable}

Syntax Description	config	Configure parameters.
	rfid auto-timeout	Configure automatic timeout of RFID tags.
	{enable disable}	Enable or disable automatic timeout.

Defaults	None.

Examples	> config rfid auto-timeout enable

Related Commands	show rfid summary config rfid status config rfid timeout

config rfid status

To configure RFID tag data collection, use the **config rfid status** command.

```
config rfid status {enable | disable}
```

Syntax Description	config	Configure parameters.
	rfid status	Configure RFID tag data collection.
	{enable disable}	Enable or disable RFID tag tracking.

Defaults None.

Examples > config rfid status enable

Related Commands show rfid summary,
 config rfid auto-timeout
 config rfid timeout

config rfid timeout

To configure the static RFID tag data timeout, use the **config rfid timeout** command.

config rfid timeout *seconds*

Syntax Description	show	Displays configurations.
	rfid timeout	Configure the static RFID tag data timeout.
	<i>seconds</i>	Timeout in seconds (from 60 to 7200).

Defaults	None.

Examples	> config rfid timeout 60

Related Commands	show rfid summary config rfid statistics

config rogue adhoc

To configure the status of an ad-hoc rogue access point (IBSS), use the **config rogue adhoc** command.

```
config rogue adhoc {acknowledged MAC | alert MAC | contain MAC num_of_APs | enable |
                    disable}
```

Syntax Description

config	Configure parameters.
rogue adhoc	Ad hoc rogue access point.
{acknowledged alert contain enable external disable}	- Enter acknowledged to acknowledge presence of a adhoc rogue. - Enter alert to generate a trap upon detection of the adhoc rogue. - Enter contain to start containing adhoc rogue. - Enter enable to enable ad-hoc rogue detection and reporting. - Enter external to set the controller to acknowledge the presence of this ad-hoc rogue. - Enter disable to disable ad-hoc rogue detection and reporting
<i>MAC</i>	MAC address of the ad-hoc rogue access point.
<i>num_of_APs</i>	The maximum number of Cisco access points to actively contain the rogue access point (1–4).

Defaults

None.

Examples

```
> config rogue adhoc acknowledge 11:11:11:11:11:11
> config rogue adhoc alert 11:11:11:11:11:11
> config rogue adhoc contain 11:11:11:11:11:11 3
> config rogue adhoc enable
> config rogue adhoc external 11:11:11:11:11:11
> config rogue adhoc disable
```

Related Commands

```
show rogue adhoc summary
show rogue adhoc detailed
config adhoc rogue
```

config rogue ap

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

```
config rogue ap {acknowledged MAC | alert MAC | known MAC | contain MAC num_of_APs |  
                  timeout timeout}
```

Syntax Description	
config	Configure parameters.
rogue ap	Rogue access point status.
{ acknowledged alert contain known timeout }	- Enter acknowledged to acknowledge presence of an access point. - Enter alert to generate a trap upon detection of the access point. - Enter contain to start containing a rogue access point. - Enter known to trust a foreign access point. - Enter timeout to specify the number of seconds after which the rogue access point and client entries expire and are removed from the list
<i>MAC</i>	MAC address of the rogue access point.
<i>num_of_APs</i>	The maximum number of Cisco access points to actively contain the rogue access point (1–4).
<i>timeout</i>	Measured in seconds between 240 and 3600

Defaults Default timeout: 1200 seconds.

Examples

```
> config rogue ap acknowledge 11:11:11:11:11:11
> config rogue ap alert 11:11:11:11:11:11
> config rogue ap contain 11:11:11:11:11:11
> config rogue ap known 11:11:11:11:11:11
> config rogue ap timeout 2000
```

Related Commands

```
show rogue ap summary
show rogue ap detailed
```

config rogue ap classify

To classify a rogue access point as friendly, malicious or unclassified, use the **config rogue ap classify** command.

```
config rogue ap classify {friendly state {internal | external} | malicious state {alert | contain} |
                        unclassified state {alert | contain} } ap_mac_address
```

Syntax Description	
config	Configure parameters.
rogue ap	Rogue access point status.
{friendly state malicious state unclassified state}	- Enter friendly state to classify a rogue access point as friendly. - Enter malicious state to classify a rogue access point as malicious. - Enter unclassified state to classify a rogue access point as unclassified.
{internal external}	- Enter internal to set the controller to trusts this rogue access point. - Enter external to set the controller to acknowledge the presence of this access point.
{alert contain}	- Enter alert to set the controller to forward an immediate alert to the system administrator for further action. - Enter contain to set the controller to contain the offending device so that its signals no longer interfere with authorized clients.
<i>ap_mac_address</i>	MAC address of the access point to be classified.

Defaults None.

Examples

```
> config rogue ap classify friendly state internal 11:11:11:11:11:11
> config rogue ap classify malicious state alert 11:11:11:11:11:11
> config rogue ap classify unclassified state contain 11:11:11:11:11:11
```

Related Commands

```
show rogue ap summary
show rogue ap detailed
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
```

config rogue ap rldp

To enable, disable, or initiate Rogue Location Discovery Protocol (RLDP), enter these commands.

```
config rogue ap rldp enable alarm-only [monitor_ap_only]
config rogue ap rldp initiate rogue_mac_address
config rogue ap rldp disable
```

Syntax Description		
config		Configure parameters.
rogue ap		Rogue access point status.
rldp		Configure RLDP.
enable alarm-only		Enable RLDP on all access points.
<i>monitor_ap_only</i>		(Optional) Enable RLDP only on access points in monitor mode.
initiate		Initiate RLDP on a specific rogue access point.
<i>rogue_mac_address</i>		MAC address of specific rogue access point.
disable		Disable RLDP on all access points.

Defaults None.

Examples

To enable RLDP on all access points, enter this command:

```
> config rogue ap rldp enable alarm-only
```

To enable RLDP on monitor-mode access point Cisco_AP_1, enter this command:

```
> config rogue ap rldp enable alarm-only Cisco_AP_1
```

To start RLDP on the rogue access point with MAC address 123.456.789.000, enter this command:

```
> config rogue ap rldp initiate 123.456.789.000
```

To disable RLDP on all access points, enter this command:

```
> config rogue ap rldp disable
```

Related Commands

```
show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue client detailed
show rogue client summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary
```

config rogue client

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

```
config rogue client {aaa {enable | disable} | alert MAC | contain MAC num_of_APs}
```

Syntax Description	config	Configure parameters.
	rogue client	Rogue client status.
	{aaa alert contain}	- Enter aaa to configure AAA server or local database to validate if rogue clients are valid clients. - Enter alert to configure the rogue client to the alarm state. - Enter contain to start containing a rogue client.
	{enable disable}	- Enter enable to enable the AAA server or local database to check MAC addresses of a rogue clients for validity. - Enter disable to disable the AAA server or local database from checking MAC addresses of rogue clients for validity.
	MAC	MAC address of the rogue client.
	num_of_APs	The maximum number of Cisco access points to actively contain the rogue access point (1–4).

Defaults None.

```
Examples
> config rogue client aaa enable
> config rogue client aaa disable
> config rogue client alert 11:11:11:11:11:11
> config rogue client contain 11:11:11:11:11:11 2
```

Related Commands

show rogue client summary

show rogue client detailed, config rogue client

config rogue rule

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

```
config rogue rule {add ap priority priority classify {friendly | malicious} rule_name | classify
{friendly | malicious} rule_name | condition ap set condition_type condition_value rule_name
| {enable | delete | disable} {all | rule_name} | match {all | any} | priority priority
rule_name}
```

Syntax Description	
config	Configure parameters.
rogue rule	Configure rogue rule.
add ap	Create a new rule
{ classify condition ap set enable delete disable match priority }	- Enter classify to change the classification of a rule. - Enter condition ap set to add conditions to a rule that the rogue access point must meet. - Enter enable to enable all rules or a single specific rule. - Enter delete to delete all rules or a single specific rule. - Enter disable to disable all rules or a single specific rule. - Enter match To specify whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule. - Enter priority to change the priority of specific rule and shift others in the list accordingly.
{ all any }	- Enter all to affect all rules defined. - Enter any to effect any rule meeting certain criteria.
{ friendly malicious }	- Enter friendly to classify a rule as friendly - Enter malicious to classify a rule as malicious.
<i>condition_type</i>	The type of the condition to be configured. The condition types are listed below: client-count—Requires that a minimum number of clients be associated to the rogue access point. Valid range is 1 to 10 (inclusive) duration—Requires that the rogue access point be detected for a minimum period of time. Valid range is 0 to 3600 seconds (inclusive) managed-ssid—Requires that the rogue access point's SSID be known to the controller. no-encryption—Requires that the rogue access point's advertised WLAN does not have encryption enabled. rssi—Requires that the rogue access point have a minimum RSSI value. Valid range is -95 to -50 dBm (inclusive) ssid—Requires that the rogue access point have a specific SSID.
<i>condition_value</i>	The value of the condition. this is dependent on condition_type

<i>priority</i>	Select the priority of the rule.
<i>rule_name</i>	The name of the rule to be configured.

Defaults

None.

Examples

```
> config rogue rule add ap priority 1 classify friendly rule_1
> config rogue rule priority 2 rule_1
> config rogue rule classify friendly rule_1
> config rogue rule condition ap set rssi -50 rule_1
> config rogue rule enable rule_2
> config rogue rule delete all
> config rogue rule disable all
> config rogue rule match any rule_2
```

Related Commands`show rogue rule summary``show rogue rule detailed`

config route add

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

config route add *ip_address netmask gateway*

Syntax Description

config	Configure parameters.
route	Network route.
add	Add a route.
<i>ip_address</i>	Network IP Address.
<i>netmask</i>	The subnet mask for the network.
<i>gateway</i>	IP Address of the gateway for the route network.

Defaults

None.

Examples

```
> config route add 10.1.1.0 255.255.255.0 10.1.1.1
```

Related Commands

show route summary
config route delete

config route delete

To remove a network route from the Service Port, use the **config route delete** command.

config route delete *ip_address*

Syntax Description

config	Configure parameters.
route	Network route.
delete	Delete a route.
<i>ip_address</i>	Network IP Address.

Defaults

None.

Examples

```
> config route delete 10.1.1.0
```

Related Commands

show route all, config route add

Configure Serial Commands

Use the **config serial** commands to configure serial port settings.

config serial baudrate

To set the serial port baud rate, use the **config serial baudrate** command.

```
config serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600}
```

Syntax Description	config	Configure parameters.
	serial baudrate	Configure serial port baud rate.
	{1200 2400 4800 9600 19200 38400 57600}	Enter one of the supported connection speeds.
Defaults	9600.	
Examples	> config serial baudrate 9600	
Related Commands	config serial timeout	

config serial timeout

To set the timeout of a serial port session, use the **config serial timeout** command.

Use this command to set the timeout for a serial connection to the front of the Cisco Wireless LAN controller from 0 to 160 minutes where 0 is no timeout.

config serial timeout *minutes*

Syntax Description	config	Configure parameters.
	serial	Serial connection settings.
	timeout	Configure timeout of a serial port session.
	<i>minutes</i>	Timeout in minutes from 0 to 160. A value of 0 indicates no timeout.
Defaults	0 (no timeout).	
Examples	> config serial timeout 10	
Related Commands	config serial timeout	

config service timestamps

To enable or disable timestamps in message logs, use the **config service timestamps** command.

config service timestamps { debug | log } { datetime | disable }

Syntax Description	
config	Configure parameters.
service	Configure service settings.
timestamps	Configure timestamps.
debug	Configure timestamps in debug messages.
log	Configure timestamps in log messages.
{ datetime disable }	- Enter datetime to timestamp message logs with the standard date and time. - Enter disable to prevent message logs being timestamped.

Defaults Disabled.

Examples

```
> config service timestamps log datetime
> config service timestamps debug disable
```

Related Commands show logging

Configure CLI Sessions Commands

Use the **config sessions** commands to configure CLI session settings.

config sessions maxsessions

To configure the number of telnet CLI sessions allowed by the Cisco Wireless LAN controller, use the **config sessions maxsessions** command. Up to five sessions are possible while a setting of zero prohibits any telnet CLI sessions.

```
config sessions maxsessions session_num
```

Syntax Description	config	Configure parameters.
	sessions	Telnet CLI session parameters.
	maxsessions	Configure the number of allowed CLI sessions.
	session_num	Number of sessions from 0 to 5.

Defaults 5.

Examples > config sessions maxsessions 2

Related Commands show sessions

config sessions timeout

To configure the inactivity timeout for telnet CLI sessions, use the **config sessions timeout** command.

config sessions timeout *timeout*

Syntax Description	config	Configure parameters.
	sessions	Telnet CLI session parameters.
	timeout	Configure the inactivity timeout for telnet CLI sessions
	<i>timeout</i>	Timeout of telnet session in minutes (from 0 to 160). A value of 0 indicates no timeout.

Defaults 5.

Examples > **config sessions timeout 20**

Related Commands show sessions

Configure SNMP Community Commands

Use the **config snmp community** commands to configure SNMP community settings.

config snmp community accessmode

To modify the access mode (Read only or Read/Write) of an SNMP community, use the **config snmp community accessmode** command.

config snmp community accessmode {ro | rw} name

Syntax Description

config	Configure parameters.
snmp	SNMP parameters.
community	SNMP community parameters.
accessmode	Configure the access mode for an SNMP community.
{ro rw}	- Enter ro to specify a Read Only mode. - Enter rw to specify a Read/Write mode.
name	SNMP community name.

Defaults

Two communities are provided by default with the following parameters:

SNMP Community Name	Client IP Address	Client IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read Only	Enable
private	0.0.0.0	0.0.0.0	Read/Write	Enable

Examples

```
> config snmp community accessmode rw private
```

Related Commands

show snmp community
config snmp community mode
config snmp community create
config snmp community delete
config snmp community ipaddr

config snmp community create

To create a new SNMP community, use the **config snmp community create** command. Use this command to create a new community with the following default configuration:

config snmp community create *name*

Syntax Description

config	Configure parameters.
snmp	SNMP parameters.
community	SNMP community parameters.
create	Create a new community.
<i>name</i>	SNMP community name. Up to 16 characters.

Defaults

None.

Examples

```
> config snmp community create test
```

```
> show snmpcommunity
```

SNMP Community Name	Client IP Address	Client IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read Only	Enable
*****	0.0.0.0	0.0.0.0	Read/Write	Enable
test	0.0.0.0	0.0.0.0	Read Only	Disable

Related Commands

show snmp community

config snmp community mode

config snmp community accessmode

config snmp community delete

config snmp community ipaddr

config snmp community delete

To delete an SNMP community, use the **config snmp community delete** command.

config snmp community delete *name*

Syntax Description

config	Configure parameters.
snmp	SNMP parameters.
community	SNMP community parameters.
delete	Delete an SNMP community.
<i>name</i>	SNMP community name.

Defaults

None.

Examples

```
> 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		
config		Configure parameters.
snmp		SNMP parameters.
community		SNMP community parameters.
ipaddr		Set IP Address parameters.
<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
 > **config snmp community ipaddr 10.10.10.10.2 255.255.255.0 public**

Related Commands

- show snmp community
- config snmp community mode
- config snmp community accessmode
- config snmp community create
- config snmp community delete
- config snmp community ipaddr

config snmp community mode

To enable or disable an SNMP community, use the **config snmp community mode** command.

config snmp community mode {enable | disable} *name*

Syntax Description

config snmp community	Configure SNMP community parameters.
mode	Configure an SNMP community
{enable disable}	Enable or disable the community.
<i>name</i>	SNMP community name.

Defaults

None.

Examples

```
> config snmp community mode disable public
```

Related Commands

show snmp community
config snmp community accessmode
config snmp community create
config snmp community delete
config snmp community ipaddr

config snmp syscontact

To set the SNMP system contact name, use the **config snmp syscontact** command.

config snmp syscontact *contact*

Syntax Description	config	Configure parameters.
	snmp	SNMP parameters.
	syscontact	Set the SNMP system contact name.
	<i>contact</i>	SNMP system contact name. Up to 31 alphanumeric characters.

Defaults	None.

Examples	> config snmp syscontact Cisco WLAN Solution_administrator

Related Commands	show snmpcommunity

config snmp syslocation

To configure the SNMP system location name, use the **config snmp syslocation** command.

config snmp syslocation *location*

Syntax Description

config	Configure parameters.
snmp	SNMP parameters.
syslocation	configure the SNMP system location name.
<i>location</i>	SNMP system location name. Up to 31 alphanumeric characters.

Defaults

None.

Examples

```
> config snmp syslocation Building_2a
```

Related Commands

show snmpcommunity

Configure SNMP Trap Receiver Commands

Use the **config smp trapreceiver** commands to configure SNMP trapreceiver settings.

config snmp trapreceiver create

To add server to receive a SNMP traps, use the **config snmp trapreceiver create** command. The IP address must be valid for the command to add the new server.

config snmp trapreceiver create *name ip_address*

Syntax Description	config	Configure parameters.
	snmp	SNMP parameters.
	trapreceiver	SNMP trap server parameters.
	create	Add a new SNMP trap receiver.
	<i>name</i>	SNMP community name. Up to 16 characters.
	<i>ip_address</i>	SNMP community IP address.

Defaults	None.

Examples	> config snmp trapreceiver create test 10.1.1.1

Related Commands	show snmp trap

config snmp trapreceiver delete

To delete a server from the trap receiver list, use the **config snmp trapreceiver delete** command.

config snmp trapreceiver delete *name*

Syntax Description

config	Configure parameters.
snmp	SNMP parameters.
trapreceiver	Server to receive traps.
delete	Delete an SNMP trap receiver.
<i>name</i>	SNMP community name. Up to 16 characters.

Defaults

None.

Examples

```
> config snmp trapreceiver delete test
```

Related Commands

show snmp trap

config snmp trapreceiver mode

To send or disable sending traps to a selected server, use the **config snmp trapreceiver mode** command. This enables or disables the Cisco Wireless LAN controller from sending the traps to the selected server.

config snmp trapreceiver mode {enable | disable} name

Syntax Description	config	Configure parameters.
	snmp	SNMP parameters.
	trapreceiver	Server to receive traps.
	mode	Configure an SNMP trap receiver.
	{enable disable}	Enable or disable an SNMP trap receiver.
	name	SNMP community name.

Defaults None.

Examples `> config snmp trapreceiver mode disable server1`

Related Commands `show snmp trap`

Configure SNMP V3 User Commands

Use the **config snmp v3user** commands to configure SNMP version 3 settings.

config snmp v3user create

To create a version 3 SNMP user, use the **config snmp v3user create** command.

```
config snmp v3user create username {ro | rw} {none | hmacmd5 | hmacsha} {none | des | aescfb128} [auth_key] [encrypt_key]
```

Syntax Description

config	Configure parameters.
snmp	SNMP parameters.
v3user create	Creates a version 3 SNMP user.
<i>username</i>	Version 3 SNMP username.
{ro rw}	- Enter ro to specify a read-only user privilege. - Enter rw to specify a read-write user privilege.
{none hmacmd5 hmacsha}	- Enter none if no authentication is required. - Enter hmacmd5 to use Hashed Message Authentication Coding-Message Digest 5 (HMAC-MD5) for authentication. - Enter hmacsha to use Hashed Message Authentication Coding-Secure Hashing Algorithm (HMAC-SHA) for authentication.
{none des aes}	- Enter none if no encryption is required. - Enter des to use Cipher Block Chaining-Digital Encryption Standard (CBC-DES) encryption. - Enter aescfb128 to use Cipher Feedback Mode-Advanced Encryption Standard-128 (CFB-AES-128) encryption.
<i>[auth_key]</i>	Authentication key for the HMAC-MD5 or HMAC-SHA authentication protocol.
<i>[encrypt_key]</i>	Encryption key for the CBC-DES or CFB-AES-128 encryption protocol.

Defaults

SNMP v3 User Name AccessMode Authentication Encryption

default Read/Write HMAC-SHA CFB-AES

Examples

To add an SNMP username called “test” with read-only privileges and no encryption or authentication, enter this command:

```
> config snmp v3user create test ro none none
```

Related Commands

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	config	Configure parameters.
	snmp	SNMP parameters.
	v3user	Version 3 SNMP.
	delete	Delete a v3 user.
	<i>username</i>	Username to delete.

Defaults	None.

Examples	This will remove an SNMP user named test. <pre>> config snmp v3user delete test</pre>

Related Commands	show snmp v3user

config snmp version

To enable or disable selected SNMP versions, use the **config snmp version** command.

```
config snmp version {v1 | v2 | v3} {enable | disable}
```

Syntax Description	config	Configure parameters.
	snmp	SNMP parameters.
	version	Configure SNMP version.
	{v1 v2 v3}	Enter an SNMP version to enable or disable.
	{enable disable}	Enable or disable specified version

Defaults	All versions enabled

Examples	> config sessions timeout 20

Related Commands	show snmpversion

Configure Spanning Tree Port Commands

Use the **config spanningtree port** commands to configure spanningtree port settings.

config spanningtree port mode

To turn fast or 802.1D Spanning Tree Protocol on or off for one or all Cisco Wireless LAN controller ports, use the **config spanningtree port mode** command.



Note

When the a Cisco 4400 series wireless LAN controller is configured for port redundancy, Spanning Tree Protocol must be disabled for all ports on the Cisco 4400 series wireless LAN controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 series wireless LAN controller.

Note that you must disable Cisco Wireless LAN controller STP using the config spanningtree switch mode command, select STP mode for all Ethernet ports using this command, and then enable Cisco Wireless LAN controller STP using the config spanningtree switch mode command. This procedure allows the Cisco Wireless LAN controller to most efficiently set up STP, detect logical network loops, place redundant ports on standby, and build a network with the most efficient pathways.

config spanningtree port mode {off | 802.1d | fast} {port | all}

Syntax Description

config	Configure parameters.
spanningtree	Spanning Tree Protocol.
port	Configure spanning tree values on a per port basis.
mode	Configure the STP port mode.
{off 802.1d fast}	Enter a supported port mode or off to disable STP for the specified ports.
{port all}	Enter a port number (1 through 12 or 1 through 24), or all to configure all ports.

Defaults

Port STP = off.

Examples

To disable STP for all Ethernet ports:

```
> config spanningtree port mode off all
```

To turn on STP 802.1D mode for Ethernet port 24:

```
> config spanningtree port mode 802.1d 24
```

To turn on fast STP mode for Ethernet port 2:

```
> config spanningtree port mode fast 2
```

Related Commands

show spanningtree port
 config spanningtree switch mode
 config spanningtree port pathcost
 config spanningtree port priority

config spanningtree port pathcost

To set the STP path cost for an Ethernet port, use the **config spanningtree port pathcost** command.



Note

When the a Cisco 4400 series wireless LAN controller is configured for port redundancy, Spanning Tree Protocol must be disabled for all ports on the Cisco 4400 series wireless LAN controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 series wireless LAN controller.

config spanningtree port pathcost {*cost* | **auto**} {*port* | **all**}

Syntax Description

config	Configure parameters.
spanningtree	Spanning Tree Protocol.
port	Configure spanning tree values on a per port basis.
pathcost	Configure the STP port path cost.
{ <i>cost</i> auto }	Enter cost in decimal as determined by the network planner or auto (default cost).
{ <i>port</i> all }	Enter a port number (1 through 12 or 1 through 24), or all to configure all ports.

Defaults

auto.

Examples

To have the STP algorithm automatically assign a path cost for all ports:

```
> config spanningtree port pathcost auto all
```

To have the STP algorithm use a port cost of 200 for port 22:

```
> config spanningtree port pathcost 200 22
```

Related Commands

show spanningtree port
config spanningtree port mode
config spanningtree port priority

config spanningtree port priority

To configure the STP port priority, use the **config spanningtree port priority** command.



Note

When the a Cisco 4400 series wireless LAN controller is configured for port redundancy, Spanning Tree Protocol must be disabled for all ports on the Cisco 4400 series wireless LAN controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 series wireless LAN controller.

config spanningtree port priority *priority_num* *port*

Syntax Description

config	Configure parameters.
spanningtree	Spanning Tree Protocol.
port	Configure spanning tree values on a per port basis.
priority	Configure the STP port priority.
<i>priority_num</i>	Enter a priority number from 0 to 255.
<i>port</i>	Enter a port number (1 through 12 or 1 through 24).

Defaults

STP Priority = 128.

Examples

To set Ethernet port 2 to STP priority 100:

```
> config spanningtree port priority 100 2
```

Related Commands

show spanningtree port
 config spanningtree switch mode
 config spanningtree port mode
 config spanningtree port pathcost

Configure Spanning Tree Switch Commands

Use the **config spanningtree switch** commands to configure spanning tree switch settings.

config spanningtree switch bridgepriority

To set the bridge ID, use the **config spanningtree switch bridgepriority** command. 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.

**Note**

When the a Cisco 4400 series wireless LAN controller is configured for port redundancy, Spanning Tree Protocol must be disabled for all ports on the Cisco 4400 series wireless LAN controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 series wireless LAN controller.

config spanningtree switch bridgepriority *priority_num*

Syntax Description

config	Configure parameters.
spanningtree	Spanning Tree Protocol.
switch	Configure spanning tree values on a per switch basis.
bridgepriority	Configure the STP bridge priority.
<i>priority_num</i>	Enter a priority number between 0 and 65535.

Defaults

The factory default is 32768.

Examples

```
> config spanningtree switch bridgepriority 40230
```

Related Commands

show spanningtree switch
config spanningtree switch forwarddelay
config spanningtree switch hellotime
config spanningtree switch maxage
config spanningtree switch mode

config spanningtree switch forwarddelay

To set the bridge timeout, use the **config spanningtree switch forwarddelay** command.

The value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Maximum Age. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent may return a badValue error if a set is attempted to a value which is not a whole number of seconds. The Factory default is 15. Valid values are 4 through 30 seconds.

config spanningtree switch forwarddelay *seconds*

Syntax Description		
config		Configure parameters.
spanningtree		Spanning Tree Protocol.
switch		Configure spanning tree values on a per switch basis.
forwarddelay		Configure the STP bridge forward delay.
<i>seconds</i>		Timeout in seconds (between 4 and 30).

Defaults The factory default is 15.

Examples > **config spanningtree switch forwarddelay 20**

Related Commands

- show spanningtree switch
- config spanningtree switch bridgepriority
- config spanningtree switch hellotime
- config spanningtree switch maxage
- config spanningtree switch mode

config spanningtree switch hellotime

To set the hello time, use the **config spanningtree switch hellotime** command.

This is the value all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D- 1990 to be 1 second. Valid values are 1 through 10 seconds.

config spanningtree switch hellotime *seconds*

Syntax	Description
config	Configure parameters.
spanningtree	Spanning Tree Protocol.
switch	Configure spanning tree values on a per switch basis.
hellotime	Configure the STP hello time.
<i>seconds</i>	STP hello time in seconds.

Defaults The factory default is 15.

Examples > **config spanningtree switch hellotime 4**

Related Commands

- show spanningtree switch
- spanningtree switch bridgepriority
- config spanningtree switch forwarddelay
- config spanningtree switch maxage
- config spanningtree switch mode

config spanningtree switch maxage

To set the maximum age, use the **config spanningtree switch maxage** command.

This is the value all bridges use for MaxAge when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Hello Time. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 6 through 40 seconds.

config spanningtree switch maxage *seconds*

Syntax Description		
config		Configure parameters.
spanningtree		Spanning Tree Protocol.
switch		Configure spanning tree values on a per switch basis.
maxage		Configure the STP bridge maximum age.
<i>seconds</i>		STP bridge maximum age in seconds.

Defaults The factory default is 20.

Examples > **config spanningtree switch maxage 30**

Related Commands

- show spanningtree switch
- config spanningtree switch bridgepriority
- config spanningtree switch forwarddelay
- config spanningtree switch hellotime
- config spanningtree switch mode

config spanningtree switch mode

To turn the Cisco Wireless LAN controller Spanning Tree Protocol on or off, use the **config spanningtree switch mode** command.

Note that you must disable the Cisco Wireless LAN controller STP using this command, select STP mode for all Ethernet ports using the config spanningtree port mode command, and then enable the Cisco Wireless LAN controller STP using this command. This procedure allows the Cisco Wireless LAN controller to most efficiently set up STP, detect logical network loops, place redundant ports on standby, and build a network with the most efficient pathways.

config spanningtree switch mode {enable | disable}

Syntax Description		
	config	Configure parameters.
	spanningtree	Spanning Tree Protocol.
	switch	Configure spanning tree values on a per switch basis.
	mode	Configure Spanning Tree Protocol on the switch.
	{enable disable}	Enable or disable Spanning Tree Protocol on the switch.

Defaults STP = Disabled.

Examples To support STP on all Cisco Wireless LAN controller Ports:
 > **config spanningtree switch mode enable**

Related Commands show spanningtree switch, config spanningtree switch bridgepriority, config spanningtree switch forwarddelay, config spanningtree switch hellotime, config spanningtree switch maxage, config spanningtree port mode

Configure Switch Configuration Commands

Use the **config switchconfig** commands to configure switch settings.

config switchconfig flowcontrol

To enable or disable 802.3x flow control, use the **config switchconfig flowcontrol** command.

config switchconfig flowcontrol {enable | disable}

Syntax Description	config	Configure parameters.
	switchconfig	Cisco Wireless LAN controller parameters.
	flowcontrol	Configure flow control.
	{enable disable}	Enable or disable 802.3x flow control.

Defaults	Disabled

Examples	> config switchconfig flowcontrol enable

Related Commands	show switchconfig

config switchconfig mode

To configure LWAPP transport mode for Layer 2 or Layer 3, use the **config switchconfig flowcontrol** command.

config switchconfig mode {L2 | L3}

Syntax Description	config	Configure parameters.
	switchconfig	Cisco Wireless LAN controller parameters.
	mode	Configure LWAPP transport mode to Layer 2 or Layer 3.
	{L2 L3}	Enter a transport mode: L2 for Layer 2 or L3 for Layer 3.

Defaults	L3

Examples	> config switchconfig mode L3

Related Commands	show switchconfig

config switchconfig secret-obfuscation

To enable or disable secret obfuscation, use the **config switchconfig secret-obfuscation** command.

config switchconfig secret-obfuscation {enable | disable}



Note

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.

Syntax Description

config	Configure parameters.
switchconfig	Cisco Wireless LAN controller parameters.
{enable disable}	Enable or disable secret obfuscation.

Defaults

Secrets and user passwords are obfuscated in the exported XML configuration file.

Examples

```
> config switchconfig secret-obfuscation enable
```

Related Commands

show switchconfig

config sysname

To set the Cisco Wireless LAN controller system name, use the **config sysname** command.

config sysname *name*

Syntax Description	config	Configure parameters.
	sysname	Configures the system name.
	<i>name</i>	System name. Up to 31 alphanumeric characters.

Defaults None.

Examples > **config sysname** Ent_01

Related Commands show sysinfo

Configure TACACS Commands

Use the **config tacacs** commands to configure TACACS+ settings.

config tacacs

To configure TACACS+ accounting, authentication, and authorization servers, use the **config tacacs** command.

config tacacs [acct | auth | athr]

Syntax Description

acct	(Optional) Configures a TACACS+ accounting server.
auth	(Optional) Configures a TACACS+ authentication server
athr	(Optional) Configures a TACACS+ authorization server

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

None.

Related Commands

show run-config
show tacacs summary

config tacacs acct

To configure TACACS+ accounting server settings, use the **config tacacs acct** command.

```
config tacacs acct {add server_index ip_address port type secret_key |
  delete server_index |
  disable server_index |
  enable server_index |
  retransmit-timeout server_index seconds }
```

Syntax Description	
add	(Optional) Add a new TACACS+ accounting server.
<i>server_index</i>	Specifies the TACACS+ accounting server index (1 to 3).
<i>ip_address</i>	Specifies the IP address for the TACACS+ accounting server.
<i>port</i>	Specifies the controller port used for the TACACS+ accounting server.
<i>type</i>	Specifies the type of secret key being used (ASCII or HEX).
<i>secret_key</i>	Specifies the secret key in ASCII or hexadecimal characters.
delete	(Optional) Deletes a TACACS+ server.
disable	(Optional) Disables a TACACS+ server.
enable	(Optional) Enables a TACACS+ server.
retransmit-timeout	(Optional) Changes the default retransmit timeout for the TACACS+ server.
seconds	Specifies the retransmit timeout (2 to 30 seconds).

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> config tacacs acct add 1 10.0.0.0 10 ascii 12345678
> config tacacs acct retransmit-timeout 30
> config tacacs acct enable 1
```

Related Commands

```
show run-config
show tacacs acct statistics
show tacacs summary
```

config tacacs athr

To configure TACACS+ authorization server settings, use the **config tacacs athr** command.

```
config tacacs athr {add server_index ip_address port type secret_key |
  delete server_index |
  disable server_index |
  enable server_index |
  retransmit-timeout server_index seconds }
```

Syntax Description		
add	(Optional) Add a new TACACS+ authorization server.	
<i>server_index</i>	Specifies the TACACS+ authorization server index (1 to 3).	
<i>ip_address</i>	Specifies the IP address for the TACACS+ authorization server.	
<i>port</i>	Specifies the controller port used for the TACACS+ authorization server.	
<i>type</i>	Specifies the type of secret key being used (ASCII or HEX).	
<i>secret_key</i>	Specifies the secret key in ASCII or hexadecimal characters.	
delete	(Optional) Deletes a TACACS+ server.	
disable	(Optional) Disables a TACACS+ server.	
enable	(Optional) Enables a TACACS+ server.	
retransmit-timeout	(Optional) Changes the default retransmit timeout for the TACACS+ server.	
seconds	Specifies the retransmit timeout (2 to 30 seconds).	

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> config tacacs athr add 3 10.0.0.0 4 ascii 12345678
> config tacacs athr retransmit-timeout 30
> config tacacs athr enable 3
```

Related Commands

- show run-config
- show tacacs athr statistics
- show tacacs summary

config tacacs auth

To configure TACACS+ authentication server settings, use the **config tacacs auth** command.

```
config tacacs auth {add server_index ip_address port type secret_key |
    delete server_index |
    disable server_index |
    enable server_index |
    retransmit-timeout server_index seconds }
```

Syntax Description	
add	(Optional) Add a new TACACS+ authentication server.
<i>server_index</i>	Specifies the TACACS+ authentication server index (1 to 3).
<i>ip_address</i>	Specifies the IP address for the TACACS+ authentication server.
<i>port</i>	Specifies the controller port used for the TACACS+ authentication server.
<i>type</i>	Specifies the type of secret key being used (ASCII or HEX).
<i>secret_key</i>	Specifies the secret key in ASCII or hexadecimal characters.
delete	(Optional) Deletes a TACACS+ server.
disable	(Optional) Disables a TACACS+ server.
enable	(Optional) Enables a TACACS+ server.
retransmit-timeout	(Optional) Changes the default retransmit timeout for the TACACS+ server.
seconds	Specifies the retransmit timeout (2 to 30 seconds).

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples

```
> config tacacs auth add 2 10.0.0.3 6 ascii 12345678
> config tacacs auth retransmit-timeout 30
> config tacacs auth enable 2
```

Related Commands

```
show run-config
show tacacs auth statistics
show tacacs summary
```

config tacacs all

To configure a single TACACS+ server for accounting, authentication, and authorization, use the **config tacacs all** command.

config tacacs all (*index*) (*ip_address*) (*port*) (*secret_key*)

Syntax Description	<i>index</i>	Specifies the TACACS+ server index (1 to 3).
	<i>ip_address</i>	Specifies the IP address of the TACACS+ server.
	<i>port</i>	Specifies the port used on the TACACS+ server.
	<i>secret_key</i>	Specifies the secret key in ASCII or hexadecimal characters.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples	None.

Related Commands	show run-config
	show tacacs summary

config time manual

To set the system time, use the **config time manual** command.

config time manual *MM/DD/YY HH:MM:SS*

Syntax Description

config	Command action.
time	Configures system time or servers.
manual	Configures the system time.
<i>MM/DD/YY</i>	Enter date.
<i>HH:MM:SS</i>	Enter time.

Defaults

None.

Examples

```
> config time manual 02/11/2003 15:29:00
```

Related Commands

show time

config time ntp

To set the Network Time Protocol, use the **config time ntp** command.

config time ntp {*interval seconds* | *server index ip_address*}

Syntax Description	
config	Command action.
time	Configures system time or servers.
ntp	Configures the Network Time Protocol.
interval	
{ <i>interval</i> <i>server</i> }	- Enter interval to configure the Network Time Protocol polling interval. - Enter server to configure the Network Time Protocol servers.
<i>seconds</i>	NTP polling interval in seconds (between 6800 and 604800).
<i>index</i>	NTP server index.
<i>ip_address</i>	NTP server's IP address. Use 0.0.0.0 to delete entry.

Defaults None.

Examples > **config time ntp interval 7000**

Related Commands **show time**

config time timezone

To configure the system's timezone, use the **config time timezone** command.

config time timezone { **enable** | **disable** } *delta_hours delta_mins*

Syntax Description

config	Command action.
time	Configures system time or servers.
timezone	Disables or enables daylight savings time for the system.
{enable disable}	Enable or disable daylight savings time.
<i>delta_hours</i>	Enter the local hour difference from Universal Coordinated Time (UCT).
<i>delta_mins</i>	Enter the local minute difference from UCT.

Defaults

None.

Examples

```
> config time timezone enable 2 0
```

Related Commands

show time

config time timezone location

To set the timezone location in order to have Daylight Savings Time (DST) set automatically when it occurs, use the **config time timezone location** command.

config time timezone location *location_index*

Syntax Description	config	Command action.
	time	Configures system time or servers.
	timezone	Enables daylight savings time for the system.
	location	Configure the location automatically
	<i>location_index</i>	A number representing the timezone required. The Timezones are as follows: 1. (GMT-12:00) International Date Line West 2. (GMT-11:00) Samoa 3. (GMT-10:00) Hawaii 4. (GMT-9:00) Alaska 5. (GMT-8:00) Pacific Time (US and Canada) 6. (GMT-7:00) Mountain Time (US and Canada) 7. (GMT-6:00) Central Time (US and Canada) 8. (GMT-5:00) Eastern Time (US and Canada) 9. (GMT-4:00) Atlantic Time (Canada) 10. (GMT-3:00) Buenos Aires (Argentina) 11. (GMT-2:00) Mid-Atlantic 12. (GMT-1:00) Azores 13. (GMT) London, Lisbon, Dublin, Edinburgh (default value) 14. (GMT +1:00) Amsterdam, Berlin, Rome, Vienna 15. (GMT +2:00) Jerusalem 16. (GMT +3:00) Baghdad 17. (GMT +4:00) Muscat, Abu Dhabi 18. (GMT +4:30) Kabul 19. (GMT +5:00) Karachi, Islamabad, Tashkent 20. (GMT +5:30) Colombo, Kolkata, Mumbai, New Delhi 21. (GMT +5:45) Katmandu 22. (GMT +6:00) Almaty, Novosibirsk 23. (GMT +6:30) Rangoon 24. (GMT +7:00) Saigon, Hanoi, Bangkok, Jakarta 25. (GMT +8:00) Hong Kong, Beijing, Chongqing 26. (GMT +9:00) Tokyo, Osaka, Sapporo 27. (GMT +9:30) Darwin 28. (GMT+10:00) Sydney, Melbourne, Canberra 29. (GMT+11:00) Magadan, Solomon Is., New Caledonia 30. (GMT+12:00) Kamchatka, Marshall Is., Fiji

Defaults None.

Examples

```
> config time timezone location 10
```

Related Commands

show time

Configure Trap Flag Commands

Use the **config trapflags** commands to configure trap flags settings.

config trapflags 802.11-Security

To enable or disable sending 802.11 Security related traps, use the **config trapflags 802.11-Security** command.

config trapflags 802.11-Security wepDecryptError {enable | disable}

Syntax Description	config	Configure parameters.
	trapflags	Trap parameters.
	802.11-Security	802.11 security traps flag.
	wepDecryptError	Send the WEP decrypt error to clients.
	{enable disable}	Enable or disable sending 802.11 Security related traps.

Defaults	Enabled

Examples	> config trapflags 802.11-Security wepDecryptError disable

Related Commands	show trapflags

config trapflags aaa

To enable or disable the sending of AAA server related traps, use the **config trapflags aaa** command.

```
config trapflags aaa {auth | servers} {enable | disable}
```

Syntax Description	config	Configure parameters.
	trapflags	Trap parameters.
	aaa	Configure the of sending AAA related traps.
	{auth servers}	- Enter auth to enable trap sending when AAA authentication failure occurs for mgmt user or net user or macfilter. - Enter servers to enable trap sending when No Radius servers are responding.
	{enable disable}	Enable or disable the sending of AAA server related traps.

Defaults Enabled

Examples > config trapflags aaa auth disable

Related Commands show trapflags

config trapflags ap

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

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

Syntax Description		
config		Configure parameters.
trapflags		Trap parameters.
ap		Cisco lightweight access point traps flag.
{register interfaceUp}		- Enter register to enable sending trap when a Cisco lightweight access point registers with Cisco switch. - Enter interfaceUp to enable sending trap when a Cisco lightweight access point interface (A or B) comes up.
{enable disable}		Enable or disable sending access point related traps.

Defaults Enabled

Examples > **config trapflags ap register disable**

Related Commands show trapflags

config trapflags authentication

To enable or disable sending traps on invalid SNMP access, use the **config trapflags authentication** command.

config trapflags authentication {enable | disable}

Syntax Description	config	Configure parameters.
	trapflags	Trap parameters.
	authentication	Configure trap sending on invalid SNMP access.
	{enable disable}	Enable or disable sending traps on invalid SNMP access.

Defaults	Enabled

Examples	> config trapflags authentication disable

Related Commands	show trapflags

config trapflags client

To enable or disable the sending of client related DOT11 traps, use the **config trapflags client** command.

```
config trapflags client {802.11-disassociate | 802.11-deauthenticate | 802.11-authfail |
                        802.11-assocfail | excluded} {enable | disable}
```

Syntax Description		
config		Configure parameters.
trapflags		Trap parameters.
client		Configure the sending of client related Dot11 traps.
{802.11-disassociate 802.11-deauthenticate 802.11-authfail 802.11-assocfail excluded}		- Enter 802.11-disassociate to enable the sending of Dot11 disassociation traps to clients. - Enter 802.11-deauthenticate to enable the sending of Dot11 deauthentication traps to clients. - Enter 802.11-authfail to enable the sending of Dot11 authentication fail traps to clients. - Enter 802.11-assocfail to enable the sending of Dot11 association fail traps to clients. - Enter excluded to enable the sending of excluded trap to clients.
{enable disable}		Enable or disable the sending of client related DOT11 traps.

Defaults Disabled

Examples > `config trapflags client 802.11-disassociate disable`

Related Commands show trapflags

config trapflags configsave

To enable or disable the sending of configuration saved traps, use the **config trapflags configsave** command.

```
config trapflags configsave {enable | disable}
```

Syntax Description	config	Configure parameters.
	trapflags	Trap parameters.
	configsave	Configure the sending of configuration saved traps.
	{enable disable}	Enable or disable the sending of configuration saved traps.

Defaults	Enabled

Examples	> config trapflags configsave disable

Related Commands	show trapflags

config trapflags ipsec

To enable or disable the sending of IPSec traps, use the **config trapflags ipsec** command.

```
config trapflags ipsec {esp-auth | esp-reply | invalidSPI | ike-neg | suite-neg | invalid-cookie}
                        {enable | disable}
```

Syntax Description	
config	Configure parameters.
trapflags	Trap parameters.
ipsec	IPSec trap flags.
{esp-auth esp-reply invalidSPI ike-neg suite-neg invalid-cookie}	• Enable the sending of IPSec traps when ESP authentication failure occurs. • Enable the sending of IPSec traps when ESP replay failure occurs. • Enable the sending of IPSec traps when ESP invalid SPI is detected. • Enable the sending of IPSec traps when IKE negotiation failure occurs. • Enable the sending of IPSec traps when suite negotiation failure occurs. • Enable the sending of IPSec traps when Isakamp invalid cookie is detected.
{enable disable}	Enable or disable the sending of IPSec traps.

Defaults Enabled

Examples > **config trapflags ipsec esp-auth disable**

Related Commands show trapflags

config trapflags linkmode

To enable or disable Cisco Wireless LAN controller level Link up/down trap flags, use the **config trapflags linkmode** command.

```
config trapflags linkmode {enable | disable}
```

Syntax Description	config	Configure parameters.
	trapflags	Trap parameters.
	linkmode	Configure switch-level link up/down trap flag.
	{enable disable}	Enable or disable Cisco Wireless LAN controller level Link up/down trap flags.

Defaults Enabled

Examples > config trapflags linkmode disable

Related Commands show trapflags

config trapflags multiusers

To enable or disable the sending of traps when multiple logins active, use the **config trapflags multiusers** command.

config trapflags multiusers {enable | disable}

Syntax Description

config	Configure parameters.
trapflags	Trap parameters.
multiusers	Configure trap sending when multiple logins are active.
{enable disable}	Enable or disable the sending of traps when multiple logins active.

Defaults

Enabled

Examples

> **config trapflags multiusers disable**

Related Commands

show trapflags

config trapflags rogueap

To enable or disable sending rogue access point detection traps, use the **config trapflags rogueap** command.

config trapflags rogueap {enable | disable}

Syntax Description	config	Configure parameters.
	trapflags	Trap parameters.
	rogueap	Configure rogue access point detection trap sending.
	{enable disable}	Enable or disable the sending of rogue access point detection traps.

Defaults	Enabled

Examples	> config trapflags rogueap disable

Related Commands	show trapflags

config trapflags rrm-params

To enable or disable the sending of RRM profile related traps, use the **config trapflags rrm-params** command.

config trapflags rrm-params {tx-power | channel | antenna} {enable | disable}

Syntax Description		
config		Configure parameters.
trapflags		Trap parameters.
rrm-params		RRM parameters traps flag.
{tx-power channel antenna}		- Enter tx-power to enable trap sending when RF manager automatically changes tx-power level for the Cisco lightweight access point interface. - Enter channel to enable trap sending when RF manager automatically changes channel for the Cisco lightweight access point interface. - Enter antenna to enable trap sending when RF manager automatically changes antenna for the Cisco lightweight access point interface.
{enable disable}		Enable or disable the sending of RRM profile related traps.

Defaults Enabled

Examples > **config trapflags rrm-params tx-power disable**

Related Commands show trapflags

config trapflags rrm-profile

To enable or disable the sending of RRM profile related traps, use the **config trapflags rrm-profile** command.

config trapflags rrm-profile {load | noise | interference | coverage} {enable | disable}

Syntax Description

config	Configure parameters.
trapflags	Trap parameters.
rrm-profile	RRM profile traps flag.
{load noise interference coverage}	- Enter load to enable trap sending when the load profile maintained by the RF manager fails. - Enter noise to enable trap sending when the noise profile maintained by the RF manager fails. - Enter interference to enable trap sending when the interference profile maintained by the RF manager fails. - Enter coverage to enable trap sending when the coverage profile maintained by the RF manager fails.
{enable disable}	Enable or disable the sending of RRM profile related traps.

Defaults

Enabled

Examples

```
> config trapflags rrm-profile load disable
```

Related Commands

show trapflags

config trapflags stpmode

To enable or disable the sending of spanning tree traps, use the **config trapflags stpmode** command.

config trapflags stpmode {enable | disable}

Syntax Description	config	Configure parameters.
	trapflags	Trap parameters.
	stpmode	Configure spanning tree trap sending.
	{enable disable}	Enable or disable the sending of spanning tree traps.

Defaults	Enabled

Examples	> config trapflags stpmode disable

Related Commands	show trapflags

config trapflags wps

To enable or disable wireless protection system (WPS) trap sending, use the **config trapflags wps** command.

```
config trapflags wps {enable | disable}
```

Syntax Description	config	Configure parameters.
	trapflags	Trap parameters.
	wps	Configure WPS trap sending.
	{enable disable}	Enable or disable WPS trap sending.

Defaults	Enabled

Examples	> config trapflags wps disable

Related Commands	show trapflags

Configure Watchlist Commands

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

config watchlist add

To add a watchlist entry for a wireless LAN, use the **config watchlist add** command.

```
config watchlist add {mac MAC | username username}
```

Syntax Description	config watchlist	Command action.
	add	Add a watchlist entry.
	{mac <i>MAC</i>	Enter mac and specify the MAC address of the wireless LAN.
	username <i>username</i> }	Enter username and specify the name of the user to watch.

Defaults	None.

Examples	> config watchlist add mac a5:6b:ac:10:01:6b

Related Commands	config watchlist delete config watchlist enable config watchlist disable show watchlist

config watchlist delete

To delete a watchlist entry for a wireless LAN, use the **config watchlist delete** command.

```
config watchlist delete { mac MAC | username username }
```

Syntax Description	config watchlist	Command action.
	delete	Delete a watchlist entry.
	{ mac MAC	- Enter mac and specify the MAC address of the wireless LAN to delete from the list. - Enter username and specify the name of the user to delete from the list.
	username username }	

Defaults	None.

Examples	> config watchlist delete mac a5:6b:ac:10:01:6b

Related Commands	config watchlist add config watchlist enable config watchlist disable show watchlist

config watchlist disable

To disable the client watchlist, use the **config watchlist disable** command.

config watchlist disable

Syntax Description	config	Command action.
	watchlist	Configure the client watchlist.
	disable	Disable the client watchlist.

Defaults	None.

Examples	<pre>> config watchlist disable</pre>

Related Commands	config watchlist add config watchlist delete show watchlist

config watchlist enable

To enable a watchlist entry for a wireless LAN, use the **config watchlist enable** command.

config watchlist enable

Syntax Description	config watchlist	Command action.
	watchlist	Configure the client watchlist.
	enable	Enable the client watchlist.

Defaults	None.

Examples	> config watchlist enable

Related Commands	config watchlist add
	config watchlist delete
	show watchlist

Configure Wireless LAN Commands

Use the **config wlan** commands to configure wireless LAN command settings.

config wlan 7920-support

To configure support for phones, use the **config wlan 7920-support** command.

To enable or disable 7920 support mode for phones that require client-controlled CAC—**config wlan 7920-support client-cac-limit {enable | disable} wlan_id**

To enable or disable 7920 support mode for phones that require access point-controlled CAC—**config wlan 7920-support ap-cac-limit {enable | disable} wlan_id**



Note You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

Syntax Description		
config		Configure parameters.
wlan		Wireless LAN parameters.
7920-support		Configure support for phones.
{ap-cac-limit client-cac-limit}		- Enter ap-cac-limit to support phones that expect the Cisco vendor-specific IE. - Enter client-cac-limit to support phones that expect the IEEE 802.11e Draft 6 QBSS-load.
{enable disable}		Enable or disable phone support.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 16.

Defaults None.

Examples `> config wlan 7920-support ap-cac-limit enable 8`

Related Commands `show wlan`

config wlan 802.11e

To configure 802.11e support on a wireless LAN, use the **config wlan 802.11e** command.

802.11e provides Quality of Service (QoS) support for LAN applications, which are critical for delay sensitive applications such as Voice over Wireless IP (VoWIP).

802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability and is especially well suited for use in networks that include multimedia capability.

```
config wlan 802.11e {allow | disable | require} wlan_id
```

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
802.11e	Configure 802.11e.
{allow disable require}	- Enter allow to allow 802.11e on the wireless LAN. - Enter disable to disable 802.11e on the wireless LAN. - Enter require to require 802.11e-enabled clients on the wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 16.

Defaults

None.

Examples

```
> config wlan 802.11e allow 1
```

Related Commands

show trapflags

config wlan aaa-override

To configure user policy override via AAA on a wireless LAN, use the **config wlan aaa-override** command.

When AAA override is enabled, and a client has conflicting AAA and Cisco Wireless LAN controller wireless LAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system will move clients from the default Cisco wireless LAN solution wireless LAN VLAN to a VLAN returned by the AAA server and predefined in the Cisco Wireless LAN controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system will also use QoS and ACL provided by the AAA server, as long as they are predefined in the Cisco Wireless LAN controller interface configuration. (This VLAN switching by AAA override is also referred to as Identity Networking.)

For instance, if the Corporate wireless LAN primarily uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the Operating System redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.

When AAA override is disabled, all client authentication defaults to the Cisco Wireless LAN controller authentication parameter settings, and authentication is only performed by the AAA server if the Cisco Wireless LAN controller wireless LAN do not contain any client-specific authentication parameters.

The AAA override values may come from a RADIUS server, for example.

config wlan aaa-override {enable | disable} {wlan_id | foreignAp}

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
aaa-override	Configures user policy override via AAA on a wireless LAN.
{enable disable}	Enable or disable policy override.
{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults

Disabled.

Examples

```
> config wlan aaa-override enable 1
```

Related Commands

show wlan

config wlan acl

To configure a wireless LAN access control list (ACL), use the **config wlan acl** command.

```
config wlan acl wlan_id [ acl_name | none ]
```

Syntax Description	wlan_id	Specifies the wireless LAN identifier (1 to 16).
	acl_name	Specifies the ACL name.
	none	Clears the ACL settings for the specified wireless LAN.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples > config wlan acl 1 office_1

Related Commands show wlan

config wlan apgroup nac

To enable or disable NAC out-of-band support for a specific AP group VLAN, enter this command:

```
config wlan apgroup nac {enable | disable} apgroup_name wlan_id
```

Syntax Description	<i>apgroup_name</i>	AP group name.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.

Defaults	Disabled.

Examples	> config wlan apgroup nac enable apgroup 4

Related Commands	config guest-lan nac config wlan nac

config wlan broadcast-ssid

To configure an SSID broadcast on a wireless LAN, use the **config wlan broadcast-ssid** command.

```
config wlan broadcast-ssid {enable | disable} wlan_id
```

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	broadcast-ssid	Configure an SSID broadcast on a wireless LAN.
	{enable disable}	Enable or disable SSID broadcasts on a wireless LAN.
	wlan_id	Wireless LAN identifier between 1 and 16.

Defaults	Disabled.

Examples	> config wlan broadcast-ssid enable 1

Related Commands	show wlan

config wlan create

To create a wireless LAN, use the **config wlan create** command.

```
config wlan create {[wlan_id] [profile_name | foreignAp] [ssid]}
```

Syntax Description	<i>wlan_id</i>	Specifies the wireless LAN identifier (between 1 and 16). Also enter the SSID network name (up to 32 alphanumeric characters). Enter foreignAp for third party access points.
	<i>profile_name</i>	Specifies a unique profile name (up to 32 alphanumeric characters). Note If an SSID is not specified, this field is used as the SSID.
	foreignAp	Specifies a foreign access point.
	<i>ssid</i>	(Optional) Specifies a unique name (up to 32 alphanumeric characters) to be used as the SSID.

Defaults	None.

Command History	Release	Modification
	4.1	This command was revised to add the optional SSID field.

Examples	> config wlan create 1 factory SSID01

Related Commands	show trapflags

config wlan delete

To delete a wireless LAN, use the **config wlan delete** command.

```
config wlan delete {wlan_id | foreignAp}
```

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	delete	Delete a wireless LAN.
	{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults	None.

Examples	> config wlan delete 16

Related Commands	show wlan
	show wlan summary

config wlan dhcp_server

To configure the internal DHCP server for a wireless LAN, use the **config wlan dhcp_server** command.

config wlan dhcp_server {*wlan_id* | **foreignAp**} *ip_address* [**required**]

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	dhcp_server	Configure internal DHCP server.
	{ <i>wlan_id</i> foreignAp }	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.
	<i>ip_address</i>	IP Address of the internal DHCP server (this parameter is required).
	[required]	Optionally, specify whether DHCP address assignment is required.

Defaults None.

Examples > **config wlan dhcp_server 16 10.10.2.1**

Related Commands show wlan

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	<i>wlan_id</i>	Specifies the wireless LAN identifier (1 to 16).
	enable	(Optional) Enables the wireless LAN diagnostic channel.
	disable	(Optional) Disables the wireless LAN diagnostic channel.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples	> config wlan diag-channel enable 1

Related Commands	show run-config
	show wlan

config wlan disable

To disable a wireless LAN, use the **config wlan disable** command.

config wlan disable {*wlan_id* | **foreignAp**}

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	disable	Disable a wireless LAN.
	{ <i>wlan_id</i> foreignAp }	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults	None.

Examples	> config wlan disable 16

Related Commands	show wlan

config wlan dtim

To disable a wireless LAN, use the **config wlan disable** command.

```
config wlan dtim {802.11a | 802.11b} dtim wlan_id
```

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	dtim	Delivery traffic indication map
	{802.11a 802.11b}	- Configure dtim for 802.11a radio network. - Configure dtim for 802.11b radio network.
	dtim	Value for dtim (between 1 - 255 inclusive)
	wlan_id	Number of the WLAN to be configured

Defaults Default dtim 1.

Examples > config wlan dtim 802.11a 128 1

Related Commands show wlan

config wlan enable

To enable a wireless LAN, use the **config wlan enable** command.

config wlan enable {*wlan_id* | **foreignAp**}

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	enable	Enable a wireless LAN.
	{ <i>wlan_id</i> foreignAp }	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults	None.

Examples	> config wlan enable 16

Related Commands	show wlan

config wlan exclusionlist

To configure the wireless LAN exclusion list, use the config wlan exclusionlist command.

```
config wlan exclusionlist [ wlan_id [enabled | disabled | time ] |  
foreignap [ enabled | disabled | time ]
```

Syntax Description

<i>wlan_id</i>	Specifies the wireless LAN identifier (1 to 16).
enabled	Enables the exclusion list for the specified wireless LAN or foreign access point.
disabled	Disables the exclusion list for the specified wireless LAN. or a foreign access point.
<i>time</i>	Specifies the exclusion list timeout in seconds. A value of zero (0) specifies infinite time.
foreignap	Specifies a third party access point.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> config wlan exclusionlist 1 enabled
```

Related Commands

```
show wlan  
show wlan summary
```

config {wlan | guest-lan} disable

To disable the WLAN or wired guest LAN for which you are configuring mobility anchors, use the **config {wlan | guest-lan} disable** command.

```
config {wlan | guest-lan} disable {wlan_id | guest_lan_id}
```

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
guest-lan	Indicates the active wired guest LAN.
disable	Disable a wireless LAN.
<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 16.
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Defaults

None.

Examples

```
> config {wlan|guest-lan} disable 5
```

Related Commands

```
config mobility group anchor add {wlan | guest-lan}
config {wlan | guest-lan} mobility anchor add
config mobility group keepalive count
config mobility group keepalive interval
config mobility group anchor delete {wlan | guest-lan}
config {wlan | guest-lan} mobility anchor delete
```

config {wlan | guest-lan} mobility anchor add

To create a new mobility anchor for the WLAN or wired guest LAN, use the **config {wlan | guest-lan} mobility anchor add** command.

```
config {wlan | guest-lan} mobility anchor add {wlan_id | guest_lan_id}
    anchor_controller_ip_address
```



Note You can also use the **config mobility group anchor add {wlan | guest-lan} {wlan_id | guest_lan_id} anchor_controller_ip_address** command.



Note The *wlan_id* or *guest_lan_id* must exist and be disabled, and the *anchor_controller_ip_address* must be a member of the default mobility group.



Note Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor.

Syntax Description

config	Configure parameters.
mobility group	Mobility group member.
wlan	Wireless LAN parameters.
guest-lan	Indicates the active wired guest LAN.
add	Add a wireless LAN or a wired guest LAN.
<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 16.
<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
<i>anchor_controller_ip_address</i>	IP address of the anchor controller.

Defaults

None.

Examples

```
> config {wlan|guest-lan} mobility anchor add 5 255.255.255.0
```

Related Commands

```
config mobility group anchor add {wlan | guest-lan}
config mobility group keepalive count
config mobility group keepalive interval
config mobility group anchor delete {wlan | guest-lan}
config {wlan | guest-lan} mobility anchor delete
```

config {wlan | guest-lan} mobility anchor delete

To delete a new mobility anchor for the WLAN or wired guest LAN, use the **config mobility group anchor delete {wlan | guest-lan}** command.

```
config {wlan | guest-lan} mobility anchor delete {wlan_id | guest_lan_id}
anchor_controller_ip_address
```



Note You can also use the **config mobility group anchor delete {wlan | guest-lan} {wlan_id | guest_lan_id} anchor_controller_ip_address** command.



Note The *wlan_id* or *guest_lan_id* must exist and be disabled.



Note Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.

Syntax Description

config	Configure parameters.
mobility group	Mobility group member.
wlan	Wireless LAN parameters.
guest-lan	Indicates the active wired guest LAN.
delete	delete a wireless LAN or a wired guest LAN.
<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 16.
<i>guest_lan_id</i>	Guest LAN indentifier between 1 and 5 (inclusive).
<i>anchor_controller_ip_a ddress</i>	IP address of the anchor controller.

Defaults

None.

Examples

```
> config {wlan|guest-lan} mobility anchor delete 5 255.255.255.0
```

Related Commands

```
config mobility group anchor add {wlan | guest-lan}
config mobility group keepalive count
config mobility group keepalive interval
config mobility group anchor delete {wlan | guest-lan}
config {wlan | guest-lan} mobility anchor delete
```

config wlan h-reap local switching

To configure the WLAN for local switching, use the **config wlan h-reap local switching** command.

```
config wlan h-reap local switching {enable | disable} wlan_id
```

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	h-reap	Hybrid REAP.
	local switching	Indicates that data packets are switched locally.
	{enable disable}	Enable or disable local switching on a wireless LAN.
	wlan_id	Wireless LAN identifier between 1 and 16.

Defaults Disable.

Examples > config wlan h-reap local switching enable 6

Related Commands show wlan

config wlan interface

To configure a wireless LAN interface, use the **config wlan interface** command.

config wlan interface { *wlan_id* | **foreignAp** } *interface-name*

Syntax Description	<i>wlan_id</i>	(Optional) Specifies the wireless LAN identifier (1 to 16)
	foreignAp	(Optional) Specifies third party access points.
	<i>interface-name</i>	Specifies the interface name.

Defaults	None.

Examples	> config wlan interface 16 VLAN901

Related Commands	show wlan

config wlan IPv6Support

To configure IPv6 support on a wireless LAN, use the **config wlan IPv6Support** command.

```
config wlan IPv6support {enable | disable} wlan_id
```

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	IPv6support	Configure IPv6 support on a wireless LAN.
	{enable disable}	Enable or disable IPv6 support on a wireless LAN.
	wlan_id	Wireless LAN identifier between 1 and 16.

Defaults None.

Examples > config wlan IPv6support enable 6

Related Commands show wlan

config wlan mac-filtering

To change the state of MAC filtering on a wireless LAN, use the **config wlan mac-filtering** command.

config wlan mac-filtering {enable | disable} {wlan_id | foreignAp}

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	mac-filtering	Configure MAC filtering on a wireless LAN.
	{enable disable}	Enable or disable MAC filtering on a wireless LAN.
	{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults	None.

Examples	> config wlan mac-filtering enable 1

Related Commands	show wlan

config wlan mfp

To configure management frame protection (MFP) options for the wireless LAN, use the **config wlan mfp** command.

```
config wlan mfp {client [enable | disable ] wlan_id |
infrastructure protection [ enable | disable ] wlan_id }
```

Syntax Description	client	(Optional) Configures client MFP for the wireless LAN.
	enable	Enables the feature.
	disable	Disables the feature.
	wlan_id	Specifies the wireless LAN identifier (1 to 16).
	infrastructure protection	(Optional) Configures infrastructure MFP for the wireless LAN.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples > config wlan mfp client enable 1

Related Commands

- show run-config
- show wlan summary
- show wlan

config wlan mobility

To change the state of MAC filtering on a wireless LAN, use the **config wlan mobility anchor** command.

config wlan mobility anchor {add | delete} *wlan_id ip_address*

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	mobility anchor	Configure the Mobility wireless LAN anchor list.
	{add delete}	Enable or disable MAC filtering on a wireless LAN.
	<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 16.
	<i>ip_address</i>	Member switch IP address for anchoring the wireless LAN.

Defaults None.

Examples > config wlan mobility anchor delete 1 192.12.1.3

Related Commands show wlan

config wlan nac

To enable or disable NAC out-of-band support for a WLAN, enter this command:

```
config wlan nac {enable | disable} wlan_id
```

Syntax Description	config	Command action.
	wlan	WLAN parameters.
	nac	NAC out-of-band support.
	enable disable	Enable or disable NAC out-of-band support.
	wlan_id	The WLAN identifier between 1 and 16.

Defaults	None

Examples	>config wlan nac enable 13

Related Commands	config guest-lan nac

config wlan peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **config wlan peer-blocking** command.

config wlan peer-blocking {disable | drop | forward-upstream} wlan_id

Syntax Description	config	Configure parameters.
	wlan	WLAN parameters.
	peer-blocking	Configures a WLAN for peer-to-peer blocking.
	{disable drop forward-upstream}	- Enter disable to disable peer-to-peer blocking and bridge traffic locally within the controller whenever possible. - Enter drop to cause the controller to discard the packets. - Enter forward-upstream to cause the packets to be forwarded on the upstream VLAN. The device above the controller decides what action to take regarding the packets.
	<i>wlan_id</i>	The WLAN identifier between 1 and 16.

Defaults **config wlan peer-blocking disable** *wlan_id*

Examples **> config wlan peer-blocking disable 1**

Related Commands **show wlan**

config wlan qos

To change the quality of service for a wireless LAN, use the **config wlan qos** command.

```
config wlan qos wlan_id {bronze | silver | gold | platinum}

config wlan qos foreignAp {bronze | silver | gold | platinum}
```

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	qos	Quality of service.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.
	foreignAp	Enter foreignAp for third party access points.
	{bronze silver gold platinum}	Enter QoS policy: bronze , silver , gold , or platinum .

Defaults	Silver.

Examples	To set the highest level of service on wireless LAN 1, use the following command: > config wlan qos 1 gold

Related Commands	show wlan

config wlan radio

To set the Cisco radio policy on a wireless LAN, use the **config wlan radio** command.

config wlan radio *wlan_id* {all | 802.11a | 802.11bg | 802.11g | 802.11ag}

Syntax Description	
config	Configure parameters.
wlan	Wireless LAN parameters.
radio	Configure the Cisco radio policy.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.
{all 802.11a 802.11bg 802.11g 802.11ag}	- Enter all to configure the wireless LAN on all radio bands. - Enter 802.11a to configure the wireless LAN on only 802.11a. - Enter 802.11bg to configure the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled). - Enter 802.11g to configure the wireless LAN on 802.11g only. - Enter 802.11ag to configure the wireless LAN on 802.11a and 802.11g only.

Defaults None.

Examples > config wlan radio 1 all

Related Commands

- config 802.11a enable
- config 802.11a disable
- config 802.11b enable
- config 802.11b disable
- config 802.11b 11gSupport enable
- config 802.11b 11gSupport disable
- show wlan

config wlan radius_server

To configure a wireless LAN's radius servers, use the **config wlan radius_server** command.

```
config wlan radius_server {auth | acct} {enable wlan_id | disable wlan_id} {add wlan_id
server_id | delete wlan_id {all | server_id}}
```

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
radius-server	RADIUS servers.
{auth acct}	Configures a RADIUS authentication or accounting server.
{enable disable}	Enable or disable RADIUS authentication or accounting for this WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
{add delete}	Add or delete a link to a configured RADIUS Server.
<i>server_id</i>	RADIUS Server Index.
all	Enter all to delete all links to configured RADIUS servers.

Defaults

None.

Examples

```
> config wlan radius_server auth add 1 1
> config wlan radius_server auth delete 1 1
> config wlan radius_server auth delete 1 all
```

Related Commands

```
config 802.11a enable
config 802.11a disable
config 802.11b enable
config 802.11b disable
config 802.11b 11gSupport enable
config 802.11b 11gSupport disable
show wlan
```

Configure Wireless LAN Security Commands

Use the **config wlan security** commands to configure wireless LAN security settings.

config wlan security 802.1X

To change the state of 802.1X security on the wireless LAN Cisco radios, use the **config wlan security 802.1X** command.

Use to change the encryption level of 802.1X security on the wireless LAN Cisco radios to:

- 40/64 bit key
- 104/128 bit key
- 128/152 bit key

```
config wlan security 802.1X {enable {wlan_id | foreignAp} | disable {wlan_id | foreignAp} |
  encryption {wlan_id | foreignAp} {40 | 104 | 128}}
```

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
802.1X	Configure 802.1X security.
{enable disable encryption}	• Enter disable to disable 802.1X. • Enter enable to enable 802.1X. • Enter encryption to set the static WEP keys and indexes.
{wlan_id foreignAp}	• Enter a wireless LAN identifier between 1 and 16. • Enter foreignAp for third party access points.
{40 104 128}	If you're setting the static WEP keys and indexes using the config wlan security 802.1X encryption command, enter a WEP key size of either 40, 104, or 128 bits.
	
Note	All keys within a wireless LAN must be same size.

Defaults

None.

Examples

```
> config wlan security 802.1X enable 16
```

Related Commands

show wlan

config wlan security ckip

Use this command to configure CKIP security options for the wireless LAN:

```
config wlan ckip [ akm | mmh | kp | disable | enable ]
```

Syntax Description	akm	(Optional) Configures key management for the CKIP wireless LAN.
	mmh	(Optional) Configures MMH MIC validation for the CKIP wireless LAN
	kp	(Optional) Configures key-permutation for the CKIP wireless LAN
	disable	(Optional) Disables CKIP security.
	enable	(Optional) Enables CKIP security.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

config wlan security tkip

To configure Temporary Key Integrity Protocol (TKIP) MIC counter measure activation timeout period, use the **config wlan security tkip hold-down** command.

```
config wlan security tkip hold-down
```

Syntax Description	hold-down	Time in seconds for which you want to activate the timeout. The range is 0–60 seconds.
		If you set the timeout to a value that is greater than zero (0) and if a TKIP MIC failure occurs within the set period, the TKIP countermeasure will be activated. If you set it to zero (0), the countermeasure action will not be activated.

Defaults 60 seconds.

Examples > config wlan security tkip hold-down 60

config wlan security cond-web-redir

To enable or disable conditional web redirect, enter this command.

```
config wlan security cond-web-redir {enable | disable} wlan_id
```

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
cond-web-redir	Configure conditional web redirect
{enable disable}	- Enter enable to enable conditional web redirect. - Enter disable to disable conditional web redirect.
<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 16.

Defaults

None.

Examples

```
> config wlan security cond-web-redir enable 2
```

Related Commands

show wlan
show wlan *wlan_id*.

config wlan security splash-page-web-redir

To enable or disable splash page web redirect, enter this command.

```
config wlan security splash-page-web-redir {enable | disable} wlan_id
```

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
splash-page-web-redir	Configure splash page web redirect
{enable disable}	- Enter enable to enable splash page web redirect. - Enter disable to disable splash page web redirect.
<i>wlan_id</i>	Enter a wireless LAN identifier between 1 and 16.

Defaults

Disabled.

Examples

```
> config wlan security splash-page-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	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Configure the wireless LAN security policy.
	ipsec disable	Disable IPSec.
	{ <i>wlan_id</i> foreignAp }	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults	None.

Examples	> config wlan security IPSec disable 16

Related Commands	show wlan

config wlan security ipsec enable

To enable IPSec security, use the **config wlan security ipsec enable** command.

```
config wlan security ipsec enable {wlan_id | foreignAp}
```

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Configure the wireless LAN security policy.
	ipsec enable	Enable IPSec.
	{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults	None.

Examples	> config wlan security IPSec enable 16

Related Commands	show wlan

config wlan security ipsec authentication

To modify the IPSec security authentication protocol used on the wireless LAN, use the **config wlan security ipsec authentication** command.

config wlan security ipsec authentication {hmac-md5 | hmac-sha-1} {wlan_id | foreignAp}

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Configure the wireless LAN security policy.
	ipsec authentication	Configure IPSec security authentication parameter.
	{hmac-md5 hmac-sha-1}	Enter the IPSec HMAC-MD5 or IPSec HMAC-SHA-1 authentication protocol.
	{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults None.

Examples
 > config wlan security ipsec authentication hmac-sha-1 1

Related Commands show wlan

config wlan security ipsec encryption

To modify the IPSec security encryption protocol used on the wireless LAN, use the **config wlan security ipsec encryption** command.

```
config wlan security ipsec encryption {3des | aes | des} {wlan_id | foreignAp}
```

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
ipsec	IPSec security.
encryption	Encryption parameter.
{3des aes des}	Enable IPSec DES encryption, IPSec AES 128-bit encryption, or IPSec 3DES encryption.
{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults

None.

Examples

```
> config wlan security ipsec encryption aes 1
```

Related Commands

show wlan

config wlan security ipsec config

To configure the propriety IKE CFG-Mode parameters used on the wireless LAN, use the **config wlan security ipsec config** command.

IKE is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how the data should be protected. IKE keeps track of connections by assigning a bundle of Security Associations (SAs), to each connection.

config wlan security ipsec config qotd *ip_address* {*wlan_id* | **foreignAp**}

Syntax Description		
config		Configure parameters.
wlan		Configure wireless LAN parameters.
security		Configure the wireless LAN security policy.
ipsec		Configure IPSec security.
config		Configure proprietary IKE CFG-MODE parameters.
qotd		Configure quote-of-the-day server IP for cfg-mode.
<i>ip_address</i>		quote-of-the-day server IP for cfg-mode.
{ <i>wlan_id</i> foreignAp }		- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults None.

Examples

```
> config wlan security ipsec config qotd 44.55.66.77 1
```

Related Commands show wlan

config wlan security ipsec ike authentication

To modify the IPSec ike authentication protocol used on the wireless LAN, use the **config wlan security ipsec ike authentication** command.

```
config wlan security ipsec ike authentication {certificates {wlan_id | foreignAp} |
pre-share-key {wlan_id | foreignAp} key | xauth-psk {wlan_id | foreignAp} key}
```

Syntax Description	
config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
ipsec	IPSec security.
ike	IKE protocol.
authentication	Authentication parameter.
{certificates pre-share-key xauth-psk}	- Enter certificates to enable IKE certificate mode. - Enter pre-share-key to enable IKE Xauth with pre-shared keys. - Enter xauth-psk to enable IKE Pre-Shared Key.
{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.
key	Key required for pre-share and xauth-psk.

Defaults None.

Examples > config wlan security ipsec ike authentication certificates 16

Related Commands show wlan

config wlan security ipsec ike dh-group

To modify the IPSec IKE Diffie Hellman group used on the wireless LAN, use the **config wlan security ipsec ike authentication** command.

config wlan security ipsec ike dh-group {*wlan_id* | **foreignAp**} {**group-1** | **group-2** | **group-5**}

Syntax Description	
config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
ipsec	Configure IPSec security.
ike	Configure the IKE protocol.
dh-group	Diffie Hellman group parameter.
{ <i>wlan_id</i> foreignAp }	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.
{ group-1 group-2 group-5 }	- Enter group-1 to specify DH group 1 (768 bits). - Enter group-2 to specify DH group 2 (1024 bits). - Enter group-5 to specify DH group 5 (1536 bits).

Defaults None.

Examples > **config wlan security ipsec ike dh-group 1 group-1**

Related Commands show wlan

config wlan security ipsec ike lifetime

To modify the IPSec IKE lifetime used on the wireless LAN, use the **config wlan security ipsec ike lifetime** command.

```
config wlan security ipsec ike lifetime {wlan_id | foreignAp} seconds
```

Syntax Description

config	Configure parameters.
wlan	Configure wireless LAN parameters.
security	Configure the wireless LAN security policy.
ipsec	Configure IPSec security.
ike	Configure IKE protocol.
lifetime	Configure IKE timeout.
{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.
seconds	The IKE lifetime in seconds, between 1800 and 345600.

Defaults

None.

Examples

```
> config wlan security ipsec ike lifetime 1 1900
```

Related Commands

show wlan

config wlan security ipsec ike phase1

To modify IPSec IKE Phase 1 used on the wireless LAN, use the **config wlan security ipsec ike phase1** command.

```
config wlan security ipsec ike phase1 {aggressive | main} {wlan_id | foreignAp}
```

Syntax Description	
config	Configure parameters.
wlan	Configure wireless LAN parameters.
security	Configure the wireless LAN security policy.
ipsec	Configure IPSec security.
ike	Configure IKE.
phase1	Configure IKE's phase one mode.
{aggressive main}	- Enter aggressive to enable the IKE aggressive mode. - Enter main to enable the IKE main mode.
{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults None.

Examples

```
> config wlan security ipsec ike phase1 aggressive 16
```

Related Commands show wlan

config wlan security ipsec ike contivity

To modify Nortel's Contivity VPN client support on the wireless LAN, use the **config wlan security ipsec ike contivity** command.

config wlan security ipsec ike contivity {enable | disable} {wlan_id | foreignAp}

Syntax Description

config	Configure parameters.
wlan	Configure wireless LAN parameters.
security	Configure the wireless LAN security policy.
ipsec	Configure IPSec security.
ike	Configure IKE protocol.
contivity	Configure Nortel Contivity VPN client support.
{enable disable}	Enable or disable contivity support for this wlan.
{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults

None.

Examples

```
> config wlan security ipsec ike contivity enable 14
```

Related Commands

show wlan

config wlan security passthru

To modify the IPSec pass-through used on the wireless LAN, use the **config wlan security ipsec ike passthru** command.

```
config wlan security passthru {enable | disable} {wlan_id | foreignAp} [ip_address]
```

Syntax Description	config	Configure parameters.
	wlan	Configure wireless LAN parameters.
	security	Configure the wireless LAN security policy.
	passthru	Configure IPSec pass-through.
	{enable disable}	Enable or disable IPSec pass-through.
	{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.
	[ip_address]	If you enable security pass-through, you must specify the IP address of the IPSec gateway.

Defaults
None.

Examples
> config wlan security passthru enable 3 192.12.1.1

Related Commands
show wlan

config wlan security static-wep-key authentication

To configure static WEP key 802.11 authentication on a wireless LAN, use the **config wlan security static-wep-key authentication** command.

```
config wlan security static-wep-key authentication {shared-key | open} wlan_id
```

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Configure the wireless LAN security policy.
	static-wep-key	Configure static WEP keys on a wireless LAN.
	authentication	Authentication setting.
	{shared-key open}	- Enter shared-key to enable shared key authentication. - Enter open to enable open system authentication.
	wlan_id	Wireless LAN identifier between 1 and 16.

Defaults None.

Examples

```
> config wlan security static-wep-key authentication shared-key 1
> config wlan security static-wep-key authentication open 1
```

Related Commands show wlan

config wlan security static-wep-key disable

To disable the use of static WEP keys, use the **config wlan security static-wep-key disable** command.

config wlan security static-wep-key disable *wlan_id*

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Configure the wireless LAN security policy.
	static-wep-key	Configure static WEP keys on a wireless LAN.
	disable	Disable the use of static WEP keys.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.

Defaults	None.

Examples	> config wlan security static-wep-key disable 1

Related Commands	config wlan security wpa encryption

config wlan security static-wep-key enable

To enable the use of static WEP keys, use the **config wlan security static-wep-key enable** command.

config wlan security static-wep-key enable *wlan_id*

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Configure the wireless LAN security policy.
	static-wep-key	Configure static WEP keys on a wireless LAN.
	enable	Disable the use of static WEP keys.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.

Defaults None.

Examples > **config wlan security static-wep-key enable 1**

Related Commands **config wlan security wpa encryption**

config wlan security static-wep-key encryption

To configure the static WEP keys and indexes, use the **config wlan security static-wep-key encryption** command. Make sure to disable 802.1X before using this command.



Note

One unique WEP Key Index can be applied to each wireless LAN. As there are only four WEP Key Indexes, only four wireless LANs can be configured for Static WEP Layer 2 encryption.

```
config wlan security static-wep-key encryption wlan_id {40 | 104 | 128} {hex | ascii} key
key-index
```

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
static-wep-key	Configure static WEP keys on a wireless LAN.
encryption	Encryption setting.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.
{ 40 104 128 }	Encryption level.
{ hex ascii }	Specify whether to use hexadecimal or ASCII characters to enter key.
<i>key</i>	Enter WEP key in ascii
<i>key-index</i>	Key index (1 to 4).

Defaults

None.

Examples

```
> config wlan security static-wep-key encryption 1 40 hex 0201702001 2
```

Related Commands

show wlan

config wlan security web-auth

To change the status of Web authentication used on the wireless LAN, use the **config wlan security web** command.

```
config wlan security web-auth {acl | enable | disable} {wlan_id | foreignAp} [{acl_name | none}]
```

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
web-auth	Web authentication.
{acl enable disable}	Configure the Access Control List, or enable or disable web authentication.
{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.
[{acl_name none}]	If configuring an ACL, enter the ACL name (up to 32 alphanumeric characters) or none .

Defaults

None.

Examples

```
> config wlan security web-auth acl 1 ACL03
> config wlan security web-auth enable 1
> config wlan security web-auth disable 1
```

Related Commands

show wlan

config wlan security web-passthrough acl

To add an ACL to the wireless LAN definition, use the **config wlan security web acl** command.

config wlan security web-passthrough acl {*wlan_id* | **foreignAp**} {*acl_name* | **none**}

Syntax Description		
config		Configure parameters.
wlan		Wireless LAN parameters.
security		Configure the wireless LAN security policy.
web-passthrough		Configure the web captive portal with no authentication required.
acl		Add an ACL to the wireless LAN definition.
{ <i>wlan_id</i> foreignAp }	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.	
{ <i>acl_name</i> none }		Enter the ACL name (up to 32 alphanumeric characters) or none .

Defaults None.

Examples > **config wlan security web-passthrough acl 1 ACL03**

Related Commands **show wlan**

config wlan security web-passthrough disable

To disable web captive portal with no authentication required on a wireless LAN, use the **config wlan security web-passthrough disable** command.

config wlan security web-passthrough disable {*wlan_id* | **foreignAp**}

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
web-passthrough	Configure the web captive portal with no authentication required.
disable	Disable web captive portal with no authentication required.
{ <i>wlan_id</i> foreignAp }	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults

None.

Examples

```
> config wlan security web-passthrough disable 1
```

Related Commands

show wlan

config wlan security web-passthrough email-input

To configure web captive portal using an email address, use the **config wlan security web-passthrough email-input** command.

config wlan security web-passthrough email-input {enable | disable} {wlan_id | foreignAp}

Syntax	Description
config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
web-passthrough	Configure the web captive portal with no authentication required.
email-input	Configure web captive portal using an email address.
{enable disable}	Enable or disable web captive portal using email address.
{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults None.

Examples > **config wlan security web-passthrough email-input enable 1**

Related Commands **show wlan**

config wlan security web-passthrough enable

To enable web captive portal with no authentication required on the wireless LAN, use the **config wlan security web-passthrough enable** command.

```
config wlan security web-passthrough enable {wlan_id | foreignAp}
```

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Configure the wireless LAN security policy.
	web-passthrough	Configure the web captive portal with no authentication required.
	enable	Enable web captive portal with no authentication required.
	{wlan_id foreignAp}	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.

Defaults None.

Examples > config wlan security web-passthrough enable 1

Related Commands show wlan

config wlan security wpa1 disable

To disable WPA1, use the **config wlan security wpa1 disable** command.

config wlan security wpa1 disable *wlan_id*

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Configure the wireless LAN security policy.
	wpa1	Configure WiFi protected access.
	disable	Disable WPA1.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.

Defaults	None.

Examples	> config wlan security wpa1 disable 1

Related Commands	show wlan

config wlan security wpa1 enable

To enable WPA1, use the **config wlan security wpa1 enable** command.

config wlan security wpa1 enable *wlan_id*

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
wpa1	Configure WiFi protected access.
enable	Enable WPA1.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.

Defaults

None.

Examples

```
> config wlan security wpa1 enable 1
```

Related Commands

show wlan

config wlan security wpa1 pre-shared-key

To configure the WPA pre-shared key mode, use the **config wlan security wpa1 pre-shared-key** command.

config wlan security wpa1 pre-shared-key {enable *wlan_id* key | disable *wlan_id*}

Syntax Description		
config		Configure parameters.
wlan		Wireless LAN parameters.
security		Configure the wireless LAN security policy.
wpa1		Configure WiFi protected access.
pre-shared-key		Configure WPA pre-shared key mode (WPA-PSK).
{enable disable}		Enable or disable WPA-PSK.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 16.
<i>key</i>		WPA pre-shared key.

Defaults None.

Examples > **config wlan security wpa1 pre-shared-key enable 1 r45**

Related Commands show wlan

config wlan security wpa2 disable

To disable WPA2, use the **config wlan security wpa2 disable** command.

config wlan security wpa2 disable *wlan_id*

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
wpa2	Configure WPA2.
disable	Disable WPA2
<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.

Defaults

None.

Examples

```
> config wlan security wpa2 disable 1
```

Related Commands

show wlan

config wlan security wpa2 enable

To enable WPA2, use the **config wlan security wpa2 enable** command.

config wlan security wpa2 enable *wlan_id*

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Configure the wireless LAN security policy.
	wpa2	Configure WPA2.
	enable	Enable WPA2
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.

Defaults None.

Examples > **config wlan security wpa2 enable 1**

Related Commands show wlan

config wlan security wpa2 pre-shared-key

To configure the WPA pre-shared key mode, use the **config wlan security wpa2 pre-shared-key** command.

```
config wlan security wpa2 pre-shared-key {enable wlan_id key | disable wlan_id}
```

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
wpa2	Configure WPA2.
pre-shared-key	Configure WPA2 pre-shared key mode (WPA2-PSK).
{enable disable}	Enable or disable WPA2-PSK.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.
<i>key</i>	WPA pre-shared key.

Defaults

None.

Examples

```
> config wlan security wpa2 pre-shared-key disable 2
```

Related Commands

show wlan

config wlan security wpa2 tkip

To change the status of WPA authentication, use the **config wlan security wpa2 tkip** command.

config wlan security wpa2 tkip {enable | disable} wlan_id

Syntax Description	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Configure the wireless LAN security policy.
	wpa2	Configure WPA2.
	tkip	Configure WPA2 TKIP mode.
	{enable disable}	Enable or disable the WPA2 TKIP mode.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.

Defaults None.

Examples
> config wlan security wpa2 tkip enable 1

Related Commands show wlan

config wlan security wpa2 wpa-compat

To change the status of WPA authentication, use the **config wlan security wpa2 wpa-compat** command.

config wlan security wpa2 wpa-compat {enable | disable} *wlan_id*

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the wireless LAN security policy.
wpa2	Configure WPA2.
wpa-compat	Configure WPA compatibility mode.
{enable disable}	Enable or disable WPA compatibility mode.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 16.

Defaults

None.

Examples

```
> config wlan security wpa2 wpa-compat enable 1
```

Related Commands

show wlan

config wlan timeout

To change the timeout of wireless LAN clients, use the **config wlan timeout** command.

config wlan timeout {*wlan_id* | **foreignAp**} *seconds*

Syntax	Description
config	Configure parameters.
wlan	Wireless LAN parameters.
timeout	Configure client timeout.
{ <i>wlan_id</i> foreignAp }	- Enter a wireless LAN identifier between 1 and 16. - Enter foreignAp for third party access points.
<i>seconds</i>	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

None.

Examples

```
> config wlan timeout 1 6000
```

Related Commands

show wlan

config wlan webauth-exclude

To release the guest user IP address when the Web authentication policy time expires and exclude the guest user from acquiring an IP address for three minutes, use the **config wlan webauth-exclude** command.

```
config wlan webauth-exclude wlan_id {enable | disable}
```

Syntax Description

config	Configuration settings.
wlan	Wireless LAN settings.
webauth-exclude	Web authentication exclusion.
<i>wlan_id</i>	Specifies the wireless LAN identifier (1 to 512).
enable	Enable Web authentication exclusion.
disable	Disable Web authentication exclusion.

Command Default

Disabled.

Usage Guidelines

You can use this command for guest WLANs that are configured with Web authentication.

This command is applicable when you configure the internal DHCP scope on the controller.

By default, when the Web authentication timer expires for a guest user, the guest user can immediately reassociate with the same IP address before another guest user can acquire the IP address. If there are many guest users or limited IP address in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user's IP address is released when the Web authentication policy time expires and the guest user is excluded from acquiring an IP address for three minutes. The IP address is available for another guest user to use. After three minutes, the excluded guest user can reassociate and acquire an IP address, if available.

Examples

```
> config wlan webauth-exclude 5 enable
```

Related Commands

[config dhcp](#)

[show run-config](#)

[show wlan](#)

config wlan wmm

To configure WMM on the wireless LAN, use the **config wlan wmm** command.

config wlan wmm [**allow** | **disable** | **require**] *wlan_id*



Note 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.

Syntax Description

allow	(Optional) Allows WMM on the wireless LAN.
<i>wlan_id</i>	Specifies the wireless LAN identifier (1 to 16).
enable	(Optional) Enables WMM on the wireless LAN.
disable	(Optional) Disables WMM on the wireless LAN.
require	(Optional) Requires WMM enabled clients on the wireless LAN.

Command Default

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> config wlan wmm allow 1
> config wlan wmm require 1
```

Related Commands

```
show run-config
show running-config
show wlan
```

Configure WPS Commands

Use the **config wps** command to configure WPS settings.

config wps ap-authentication

To configure access point neighbor authentication, use the **config wps ap-authentication** command.

config wps ap-authentication [**enable** | **disable** | **threshold** *threshold_value*]

Syntax Description

enable	(Optional) Enables WMM on the wireless LAN.
disable	(Optional) Disables WMM on the wireless LAN.
threshold	(Optional) Requires WMM enabled clients on the wireless LAN.
<i>threshold_value</i>	Specifies the threshold value (1 to 255).

Command Default

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> config wps ap-authentication threshold 25
> config wps ap-authentication enable

> show wps ap-authentication summary

AP neighbor authentication is <enabled>.

Authentication alarm threshold is 10.
RF-Network Name: <doc>

> config wps ap-authentication disable

> show wps ap-authentication summary

AP neighbor authentication is <disabled>.

Authentication alarm threshold is 10.
RF-Network Name: <doc>
```

Related Commands

show wps ap-authentication summary

config wps cids-sensor

This command is used to configure IDS sensors for the WPS, use the **config wps cids-sensor** command.

```
config wps cids-sensor { [ add index ip_address username password ] | [delete index] |  
[enable index] | [disable index] | [port index port] | [interval index query_interval] |  
[fingerprint index sha1 fingerprint] }
```

Syntax Description	add	Configures a new IDS sensor.
	<i>index</i>	Specifies IDS sensor internal index.
	<i>ip_address</i>	Specifies the IDS sensor IP address.
	<i>username</i>	Specifies the IDS sensor username.
	<i>password</i>	Specifies the IDS sensor password.
	delete	Deletes an IDS sensor.
	enable	Enables an IDS sensor.
	disable	Disables an IDS sensor.
	port	Configures the IDS sensor's port number.
	<i>port</i>	Specifies the port number.
	interval	Configures the IDS sensor's query interval.
	<i>query_interval</i>	Specifies the query interval setting.
	fingerprint	Configures the IDS sensor's TLS fingerprint.
	sha1	Configures the TLS fingerprint.
	<i>fingerprint</i>	Specifies the TLS fingerprint.

[illegible]

Command History	Release	Modification
	4.1	This command was introduced.

Examples

To add a new IDS sensor to the WPS, use this command:

```
> config wps cids-sensor add 1 10.0.0.51 Sensor_user0doc1 password01
```

Related Commands	show wps cids-sensshow wps cids-sensor detail or summary

config wps mfp

To configure Management Frame Protection (MFP), use the **config wps mfp** command.

```
config wps mfp infrastructure {enable | disable}
```

Syntax Description	mfp infrastructure	Configures infrastructure MFP.
	enable disable	Enable or disable MFP.

Defaults This command has no defaults.

Examples

```
> config wps mfp infrastructure enable
> config wps mfp infrastructure disable
```

Related Commands [show wps mfp](#)

config wps rogue-ap

To configure rogue access point and rogue client policies, use the **config wps rogue-ap** command.

```
config wps rogue-ap { aaa [enable | disable] | adhoc [enable | disable] |
  rldp [enable | disable | initiate mac_address] | timeout seconds }
```

Syntax Description		
aaa	(Optional)	Validates if the rogue is a valid client using the authentication, authorization, and accounting (AAA) database or the local database.
adhoc	(Optional)	Configures ad-hoc rogue detection and reporting policies.
enable	(Optional)	Enables the feature.
disable	(Optional)	Disables the feature.
rldp	(Optional)	Configures rogue location discovery protocol (RLDP).
initiate	(Optional)	Initiates RLDP on a specified rogue access point or client.
<i>mac_address</i>		Specifies the MAC address of the rogue access point or client.
timeout	(Optional)	Configures the expiration time for rogue entries.
<i>seconds</i>		Specifies the timeout value (240 to 3600 seconds).

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	The command was revised to include the RLDP option.

Examples

```
> config wps rogue-ap timeout 1300
> config wps rogue-ap aaa enable
> config wps rogue-ap rldp initiate 32:7a:52:13:00:01
```

Related Commands show wps summary

config wps shun-list

To force the controller to sync up with other controllers in the mobility group for the shun list, enter this command:

config wps shun-list re-sync

Syntax Description	This command has no arguments or keywords

Defaults	None

Examples	> config wps shun-list re-sync

Related Commands	show wps shun-list

config wps signature

To enable or disable IDS signature processing, or to enable or disable a specific IDS signature, use the **config wps signature** command.

config wps signature {enable | disable}

config wps signature {standard | custom} state *signature_id* {enable | disable}

Syntax Description	enable disable	Enables or disables IDS signature processing or a specific IDS signature.
	standard custom	Configures a standard or custom IDS signature.
	state	Specifies the state of the IDS signature.
	<i>signature_id</i>	Specifies the identifier for the signature to be enabled or disabled.

Command Default IDS signature processing is enabled by default.

Usage Guidelines If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples To enable IDS signature processing, which enables the processing of all IDS signatures, enter this command:

```
> config wps signature enable
```

To disable a standard individual IDS signature, enter this command:

```
> config wps signature standard state 15 disable
```

Related Commands

- [config wps signature frequency](#)
- [config wps signature interval](#)
- [config wps signature mac-frequency](#)
- [config wps signature quiet-time](#)
- [config wps signature reset](#)
- [show wps signature events {standard | custom}](#)
- [show wps signature events summary](#)
- [show wps signature summary](#)
- [show wps summary](#)

config wps signature frequency

To specify the number of matching packets per interval that must be identified at the individual access point level before an attack is detected, use the **config wps signature frequency** command.

config wps signature frequency *signature_id* *frequency*

Syntax Description

frequency	Sets the frequency of the IDS signature.
<i>signature_id</i>	Specifies the identifier for the signature to be configured.
<i>frequency</i>	Sets the number of matching packets per interval that must be at the individual access point level before an attack is detected. Range: 1 to 32,000 packets per interval.

Command Default

The *frequency* default value varies per signature.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples

To set the number of matching packets per interval per access point before an attack is detected to 1800 for signature ID 4, enter this command:

```
> config wps signature frequency 4 1800
```

Related Commands

[config wps signature](#)
[config wps signature interval](#)
[config wps signature mac-frequency](#)
[config wps signature quiet-time](#)
[config wps signature reset](#)
[show wps signature events {standard | custom}](#)
[show wps signature events summary](#)
[show wps signature summary](#)
[show wps summary](#)

config wps signature interval

To specify the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval, use the **config wps signature interval** command.

config wps signature interval *signature_id* *interval*

Syntax Description	interval	Sets the interval of the IDS signature.
	<i>signature_id</i>	Specifies the identifier for the signature to be configured
	<i>interval</i>	Sets the number of seconds that must elapse before the signature frequency threshold is reached. Range: 1 to 3,600 seconds.

Command Default The default value of *interval* varies per signature.

Usage Guidelines If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples To set the number of seconds to elapse before reaching the signature frequency threshold to 200 for signature ID 1, enter this command:

```
> config wps signature interval 1 200
```

Related Commands

- config wps signature
- config wps signature frequency
- config wps signature mac-frequency
- config wps signature quiet-time
- config wps signature reset
- show wps signature events {standard | custom}
- show wps signature events summary
- show wps signature summary
- show wps summary

config wps signature mac-frequency

To specify the number of matching packets per interval that must be identified per client per access point before an attack is detected, use the **config wps signature mac-frequency** command.

config wps signature mac-frequency *signature_id* *mac_frequency*

Syntax Description

mac-frequency	Sets the MAC frequency of the IDS signature.
<i>signature_id</i>	Specifies the identifier for the signature to be configured.
<i>mac_frequency</i>	Sets the number of matching packets per interval that must be identified per client per access point before an attack is detected. Range: 1 to 32,000 packets per interval.

Command Default

The *mac_frequency* default value varies per signature.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples

To set the number of matching packets per interval per client before an attack is detected to 50 for signature ID 3, enter this command:

```
> config wps signature mac-frequency 3 50
```

Related Commands

```
config wps signature
config wps signature frequency
config wps signature interval
config wps signature quiet-time
config wps signature reset
show wps signature events {standard | custom}
show wps signature events summary
show wps signature summary
show wps summary
```

config wps signature quiet-time

To specify the length of time after which no attacks have been detected at the individual access point level and the alarm can stop, use the **config wps signature quiet-time** command.

config wps signature quiet-time *signature_id* *quiet_time*

Syntax Description	quiet-time	Sets the quiet time of the IDS signature.
	<i>signature_id</i>	Specifies the identifier for the signature to be configured.
	<i>quiet_time</i>	Sets the length of time after which no attacks have been detected at the individual access point level and the alarm can stop. Range: 60 to 32,000 seconds.

Command Default	The default value of <i>quiet_time</i> varies per signature.

Usage Guidelines	If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples	To set the number of seconds after which no attacks have been detected per access point to 60 for signature ID 1, enter this command: > config wps signature quiet-time 1 60

Related Commands	config wps signature config wps signature frequency config wps signature interval config wps signature mac-frequency config wps signature reset show wps signature events {standard custom} show wps signature events summary show wps signature summary show wps summary

config wps signature reset

To reset a specific IDS signature or all IDS signatures to default values, use the **config wps signature reset** command.

config wps signature reset {*signature_id* | **all**}

Syntax Description

reset	Resets the IDS signature.
<i>signature_id</i>	Specifies the identifier for the specific IDS signature to be reset.
all	Resets all IDS signatures.

Command Default

config wps signature reset all

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Examples

To reset the IDS signature 1 to default values, enter this command:

```
> config wps signature reset 1
```

Related Commands

[config wps signature](#)
[config wps signature frequency](#)
[config wps signature interval](#)
[config wps signature mac-frequency](#)
[config wps signature quiet-time](#)
[show wps signature events {standard | custom}](#)
[show wps signature events summary](#)
[show wps signature summary](#)
[show wps summary](#)

lwapp ap controller ip address

To configure the controller IP address into the H-REAP access point from the access point's console port, use the **lwapp ap controller ip address** command.

lwapp ap controller ip address *ip_address*



Note

This command must be entered from an access point's console port.

Syntax Description

<i>ip_address</i>	Specifies the IP address of the controller.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Prior to changing the H-REAP configuration on an access point using the access point's console port, the access point must be in standalone mode (not connected to a controller) and you must remove the current LWAPP private configuration using the **clear lwapp private-config** command.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher.

Examples

```
AP# clear lwapp private-config
removing the reap config file flash:/lwapp_reap.cfg
AP# lwapp ap controller ip address 10.92.109.1
```

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	save	Save switch configurations.
	config	Save current settings to NVRAM.

Defaults	None.

Examples	> save config
	Are you sure you want to save? (y/n) y
	Configuration Saved!

Related Commands	show sysinfo

Clearing Configurations, Logfiles, and Other Actions

To clear existing configurations, log files, and other functions, use the clear commands.

clear acl counters

To clear the current counters for an access control list (ACL), use the **clear acl counters** command.

```
clear acl counters acl_name
```



Note

ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

Syntax Description

clear acl	Command action.
counters	The number of packets hitting the ACLs configured on your controller.
<i>acl_name</i>	The name of the ACL.

Defaults

None.

Examples

```
> clear acl counters acl1
```

Related Commands

- config acl counter
- show acl detailed

clear ap-config

Use the **clear ap-config command** to clear (reset to factory default values) a lightweight access point's configuration settings.

clear ap-config *ap_name*

Syntax Description	ap_name	Specifies the access point name.

Defaults	This command has no defaults.

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

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

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

<i>ap_name</i>	Specifies the access point name.

Defaults

None.

Examples

```
> clear ap-eventlog all
This will clear event log contents for all APs. Do you want continue? (y/n) :y

Any AP event log contents have been successfully cleared.
```

Related Commands

[show ap eventlog](#)

clear arp

To clear the ARP table to a Cisco lightweight access point its factory default, use the **clear arp** command.

clear arp

Syntax Description	clear	Clear selected configuration elements.
	arp	Clear the ARP table.

Defaults	None.

Examples	<pre>> clear arp Are you sure you want to clear the ARP cache? (y/n)</pre>

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 config

To reset configuration data to factory defaults, use the **clear config** command.

clear config

Syntax Description	clear	Clear selected configuration elements.
	config	Reset configuration data to factory defaults.

Defaults	None.

Examples	> clear config
	Are you sure you want to clear the configuration? (y/n)
	n
	Configuration not cleared!

Related Commands	clear transfer
	clear download filename
	clear download mode
	clear download path
	clear download serverip
	clear download start
	clear upload datatype
	clear upload filename
	clear upload mode
	clear upload path
	clear upload serverip
	clear upload start

clear ext-webauth-url

To clear the external web authentication URL, use the **clear ext-webauth-url** command.

clear ext-webauth-url

Syntax Description	clear	Clear selected configuration elements.
	ext-webauth-url	Clear the external web authentication URL.

Defaults	None.

Examples	<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 location rfid

To clear a specific RFID tag or all of the RFID tags in the entire database, use the **clear location rfid** command.

clear location rfid {*mac_address* | **all**}

Syntax Description

clear location rfid	Clears RFID tags.
<i>mac_address</i>	The MAC address of a specific RFID tag.
all	All of the RFID tags in the database.

Defaults

This command has no defaults.

Examples

```
> clear location rfid all
```

Related Commands

show location

clear location statistics rfid

To clear the RFID statistics, use the **clear location statistics rfid** command.

clear location statistics rfid

Syntax Description	clear	Clear selected configuration elements.
	location statistics rfid	RFID statistics.

Defaults	This command has no defaults.

Examples	> clear location statistics rfid

Related Commands	show location statistics rfid

clear locp statistics

To clear the LOCP statistics, use the **clear locp statistics** command.

clear locp statistics

Syntax Description

clear	Clears selected configuration elements.
locp statistics	Statistics related to LOCP.

Defaults

This command has no defaults.

Examples

```
> clear locp statistics
```

Related Commands

show nmsp statistics

clear lwapp private-config

Use the **clear lwapp private-config** command to clear (reset to default values) an access point's current LWAPP private configuration, which contains static IP addressing and controller IP address configurations. This command is executed from the access point console port.

clear lwapp private-config

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Usage Guidelines Prior to changing the H-REAP configuration on an access point using the access point's console port, the access point must be in standalone mode (not connected to a controller) and you must remove the current LWAPP private configuration using the **clear lwapp private-config** command.



Note

The access point must be running Cisco IOS Release 12.3(11)JX1 or higher.

Examples

```
AP# clear lwapp private-config
removing the reap config file flash:/lwapp_reap.cfg
```

Related Commands

- lwapp ap controller ip address
- debug lwapp console cli

clear radius acct statistics

To clear the radius accounting statistics on the controller, use the **clear radius acc statistics** command.

clear radius acct statistics [*index* | **all**]

Syntax Description

<i>index</i>	Specifies the index of the radius accounting server.
all	Specifies all radius accounting servers.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> clear radius acct statistics
```

Related Commands

show radius acct statistics

clear radius auth statistics

To clear the TACACS+ authentication server statistics in the controller, use the **clear tacacs auth statistics** command.

clear radius tacacs auth statistics [*index* | **all**]

Syntax Description

<i>index</i>	Specifies the index of the TACACS+ authentication server.
all	Specifies all TACACS+ authentication servers.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> clear radius auth statistics
```

Related Commands

show tacacs auth statistics
show tacacs summary
config tacacs auth

clear redirect-url

To clear the custom web authentication redirect URL on the Cisco Wireless LAN controller, use the **clear redirect-url** command.

clear redirect-url

Syntax Description	clear	Clear selected configuration elements.
	redirect-url	Clear the custom web authentication redirect URL.

Defaults None.

Examples

```
> clear redirect-url

URL cleared.
```

Related Commands

- clear transfer
- clear download datatype
- clear download filename
- clear download mode
- clear download path
- clear download start
- clear upload datatype
- clear upload filename
- clear upload mode
- clear upload path
- clear upload serverip
- clear upload start

clear stats ap wlan

To clear the WLAN statistics, use the **clear stats ap wlan** command.

```
clear stats ap wlan Cisco_AP
```

Syntax Description	Cisco_AP	Clear selected configuration elements.

Defaults	This command has no defaults.

Examples	> clear stats ap wlan cisco-ap WLAN statistics cleared.

Related Commands	show ap stats show ap wlan

clear stats local-auth

To clear the local EAP statistics, use the **clear stats local-auth** command.

clear stats local-auth

Syntax Description	clear	Clear selected configuration elements.
	stats	Clear statistics counters.
	local-auth	Clear local EAP statistics.

Defaults	This command has no defaults.

Examples	<pre>> clear stats local-auth</pre> Local EAP Authentication Stats Cleared.

Related Commands	show local-auth statistics

clear stats mobility

To clear mobility manager statistics, use the **clear stats mobility** command.

clear stats mobility

Syntax Description	clear	Clear selected configuration elements.
	stats	Clear statistics counters.
	mobility	Clear mobility manager statistics

Defaults	None.

Examples	<pre>> clear stats mobility Mobility stats cleared.</pre>

Related Commands	clear transfer clear download datatype clear download filename clear download mode clear download serverip clear download start clear upload datatype clear upload filename clear upload mode clear upload path clear upload serverip clear upload start clear stats port

clear stats port

To clear statistics counters for a specific port, use the **clear stats port** command.

clear stats port *port*

Syntax Description	clear	Clear selected configuration elements.
	stats	Clear statistics counters.
	port	Clear statistics counters for a specific port.
	<i>port</i>	Physical interface port number.

Defaults	None.

Examples	<pre>> clear stats port 9</pre>

Related Commands	clear transfer clear download datatype clear download filename clear download mode clear download serverip clear download start clear upload datatype clear upload filename clear upload mode clear upload path clear upload serverip clear upload start

clear stats radius

To clear the statistics for one or more RADIUS servers, use the **clear stats radius** command.

clear stats radius {**auth** | **acct**} {*index* | **all**}

Syntax Description

clear	Clear selected configuration elements.
stats	Clear statistics counters.
radius	Clear statistics regarding radius servers.
{ auth acct }	- Clear statistics regarding authentication. - Clear statistics regarding accounting.
{ <i>index</i> all }	- The index number of the radius server to be cleared. - Enter all to clear statistics for all radius servers.

Defaults

None.

Examples

```
> clear stats radius auth all
> clear stats radius acct all
> clear stats radius auth 2
```

Related Commands

clear transfer
clear download datatype
clear download filename
clear download mode
clear download serverip
clear download start
clear upload datatype
clear upload filename
clear upload mode
clear upload path
clear upload serverip
clear upload start

clear stats switch

To clear all switch statistics counters on a Cisco Wireless LAN controller, use the **clear stats switch** command.

clear stats switch

Syntax Description

clear	Clear selected configuration elements.
stats	Clear statistics counters.
switch	Clear all switch statistics counters.

Defaults

None.

Examples

```
> clear stats switch
```

Related Commands

clear transfer
clear download datatype
clear download filename
clear download mode
clear download path
clear download start
clear upload datatype
clear upload filename
clear upload mode
clear upload path
clear upload serverip
clear upload start

clear stats tacacs

To clear the TACACS+ server statistics on the controller, use the **clear stats tacacs** command.

```
clear stats tacacs [ auth | athr | acct ] [ index | all ]
```

Syntax Description

auth	Clears the TACACS+ authentication server statistics.
athr	Clears the TACACS+ authorization server statistics.
acct	Clears the TACACS+ accounting server statistics.
<i>index</i>	Specifies the index of the TACACS+ server.
all	Specifies all TACACS+ servers.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> clear stats tacacs acct 1
```

Related Commands

show tacacs summary

clear transfer

To clear the transfer information, use the **clear transfer** command.

clear transfer

Syntax Description	clear	Clear selected configuration elements.
	transfer	Clear the transfer information.

Defaults	None.

Examples	<pre>> clear transfer</pre> Are you sure you want to clear the transfer information? (y/n) y Transfer Information Cleared.

Related Commands	clear transfer clear download datatype clear download filename clear download mode clear download path clear download serverip clear upload datatype clear download filename clear download mode clear download path clear download serverip clear download start

clear traplog

To clear the trap log, use the **clear traplog** command.

clear traplog

Syntax Description	clear	Clear selected configuration elements.
	traplog	Clear the trap log.

Defaults	None.

Examples	> clear traplog
	Are you sure you want to clear the trap log? (y/n) y
	Trap Log Cleared.

Related Commands	clear transfer
	clear download datatype
	clear download filename
	clear download mode
	clear download path
	clear download serverip
	clear download start
	clear upload filename
	clear upload mode
	clear upload path
	clear upload serverip
	clear upload start

clear webimage

To clear the custom web authentication image, use the **clear webimage** command.

clear webimage

Syntax Description

clear	Clear selected configuration elements.
webimage	Clear the custom web authentication image.

Defaults

None.

Examples

```
> clear webimage
```

Related Commands

clear transfer
clear download datatype
clear download filename
clear download mode
clear download path
clear download serverip
clear download start
clear upload filename
clear upload mode
clear upload path
clear upload serverip
clear upload start

clear webmessage

To clear the custom web authentication message, use the **clear webmessage** command.

clear webmessage

Syntax Description	clear	Clear selected configuration elements.
	webmessage	Clear the custom web authentication message.

Defaults	None.

Examples	<pre>> clear webmessage Message cleared.</pre>

Related Commands	clear transfer
	clear download datatype
	clear download filename
	clear download mode
	clear download path
	clear download serverip
	clear download start
	clear upload filename
	clear upload mode
	clear upload path
	clear upload serverip
	clear upload start

clear webtitle

To clear the custom web authentication title, use the **clear webtitle** command.

clear webtitle

Syntax Description	clear	Clear selected configuration elements.
	webtitle	Clear the custom web authentication title.

Defaults None.

Examples

```
> clear webtitle

Title cleared.
```

Related Commands

- clear transfer
- clear download datatype
- clear download filename
- clear download mode
- clear download path
- clear download serverip
- clear download start
- clear upload filename
- clear upload mode
- clear upload path
- clear upload serverip
- clear upload start

Uploading and Downloading Files and Configurations

To transfer files to or from the Cisco Wireless LAN controller, use the transfer commands.

transfer download certpassword

To set the password for the .PEM file so that the operating system can decrypt the web administration SSL key and certificate, use the **transfer download certpassword** command.

transfer download certpassword *private_key_password*

Syntax Description

transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
certpassword	Set a certificate's private key password.
<i>private_key_password</i>	Enter a certificate's private key password or blank to clear the current password.

Defaults

None.

Examples

```
> transfer download certpassword
```

```
Clearing password
```

Related Commands

clear transfer
transfer download filename
transfer download mode
transfer download path
transfer download serverip
transfer download start
transfer upload datatype
transfer upload filename
transfer upload mode
transfer upload path
transfer upload serverip
transfer upload start

transfer download datatype

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

transfer download datatype {config | code | image | signature | webadmincert | webauthcert}

Syntax Description	
transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
datatype	Set download file type.
{config code image signature webadmincert webauthcert webauthbundle eapdevcert eapcert}	• Enter config to download configuration file. • Enter code to download an executable image to the system. • Enter image to download a web page logo to the system. • Enter signature to download a signature file to the system. • Enter webadmincert to download a certificate for web administration to the system. • Enter webauthcert to download a web certificate for web portal to the system. • Enter webauthbundle to download custom webauth bundle to the system. • Enter eapdevcert to download an EAP dev certificate to the system. • Enter eapcert to download an EAP ca certificate to the system.

Defaults None.

Examples `> transfer download datatype code`

Related Commands

- 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 start

transfer download filename

To download a specific file, use the **transfer download filename** command.

transfer download filename *webadmincert_name.pem*

Syntax Description

transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
filename	Set the FTP or TFTP filename.
<i>filename</i>	File name up to 16 alphanumeric characters.

Defaults

None.

Examples

```
> transfer download filename build603
```

Related Commands

clear transfer
transfer download datatype
transfer download mode
transfer download path
transfer download serverip
transfer download start
transfer upload datatype
transfer upload filename
transfer upload mode
transfer upload path
transfer upload serverip
transfer upload start

transfer download mode

To set transfer mode, use the **transfer download mode** command.

transfer download mode {ftp | tftp}

Syntax Description		
transfer		Transfer a file to or from the switch.
download		Transfer a file to the switch.
mode		Set transfer mode.
ftp		Set the transfer mode to ftp.
tftp		Set the transfer mode to tftp.

Defaults None.

Examples `> transfer download mode tftp`

Related Commands

- `clear transfer`
- `transfer download datatype`
- `transfer download filename`
- `transfer download path`
- `transfer download serverip`
- `transfer download start`
- `transfer upload datatype`
- `transfer upload filename`
- `transfer upload mode`
- `transfer upload path`
- `transfer upload serverip`
- `transfer upload start`

transfer download password

To set the password for FTP transfer, use the **transfer download password** command.

transfer download password *password*

Syntax Description

transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
password	Set FTP password.
<i>password</i>	Password.

Defaults

None.

Examples

```
>transfer download password pass01
```

Related Commands

[transfer download mode](#)
[transfer download port](#)
[transfer download username](#)

transfer download path

To set a specific FTP or TFTP path, use the **transfer download path** command.

transfer download path *path*

Syntax Description		
transfer		Transfer a file to or from the switch.
download		Transfer a file to the switch.
path		Set FTP or TFTP Path.
<i>path</i>		Directory path.
	Note	Pathnames on a TFTP or FTP server are relative to the server's default or root directory. For example, in the case of the Solarwinds TFTP server, the path is "/".

Defaults None.

Examples `> transfer download path c:\install\version2`

Related Commands

- clear transfer
- transfer download datatype
- transfer download filename
- transfer download mode
- transfer download serverip
- transfer download start
- transfer upload datatype
- transfer upload filename
- transfer upload mode
- transfer upload path
- transfer upload serverip
- transfer upload start

transfer download port

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

transfer download port *port*

Syntax Description

transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
port	FTP port.
<i>port</i>	Set FTP port

Defaults

The default FTP *port* is **21**.

Examples

```
>transfer download port 23
```

Related Commands

[transfer download mode](#)
[transfer download password](#)
[transfer download username](#)

transfer download serverip

To configure the IP address of the TFTP server from which to download information, use the **transfer download serverip** command.

transfer download serverip *TFTP_server ip_address*

Syntax Description	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	serverip	Enter IP address of the server.
	<i>TFTP_server</i>	TFTP IP address.
	<i>ip_address</i>	Server IP address.

Defaults None.

Examples `> transfer download serverip 175.34.56.78`

Related Commands

- clear transfer
- transfer download datatype
- transfer download filename
- transfer download mode
- transfer download path
- transfer download start
- transfer upload datatype
- transfer upload filename
- transfer upload mode
- transfer upload path
- transfer upload serverip
- transfer upload start

transfer download start

To initiate a download, use the **transfer download start** command.

transfer download start

Syntax Description	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	start	Initiate a download.

Defaults None.

Examples

```
> transfer download start

Mode..... TFTP
Data Type..... Site Cert
TFTP Server IP..... 172.16.16.78
TFTP Path..... directory path
TFTP Filename..... webadmincert_name

This may take some time.
Are you sure you want to start? (y/n) y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

Related Commands

- clear transfer**
- transfer download 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 download tftpPktTimeout

To specify the TFTP packet timeout, use the **transfer download tftpPktTimeout** command.

transfer download tftpPktTimeout *timeout*

Syntax Description	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	tftpPktTimeout	Enter the tftp packet timeout.
	<i>timeout</i>	Timeout in seconds between 1 and 254.

Defaults None.

Examples > **transfer download tftpPktTimeout 55**

Related Commands

- clear transfer
- transfer download 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 download tftpMaxRetries

To specify the number of allowed TFTP packet retries, use the **transfer download tftpMaxRetries** command.

transfer download tftpMaxRetries *retries*

Syntax Description

transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
tftpMaxRetries	Enter the number of allowed TFTP packet retries.
<i>retries</i>	Number of allowed TFTP packet retries between 1 and 254 seconds.

Defaults

None.

Examples

```
> transfer download tftpMaxRetries 55
```

Related Commands

clear transfer
transfer download 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 download username

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

transfer download username *username*

Syntax Description	transfer	Transfer a file to or from the switch.
	download	Transfer a file to the switch.
	username	FTP port.
	<i>username</i>	Set FTP port.

Defaults None.

Examples

```
>transfer download username ftp_username
```

Related Commands

- [transfer download mode](#)
- [transfer download password](#)
- [transfer download port](#)

transfer encrypt

To configure encryption for config file transfers, use the **transfer encrypt** command.

transfer encrypt {**enable** | **disable** | set-key *key*}

Syntax Description	transfer	Transfer a file to or from the switch.
	encrypt	Transfer a file to the switch.
	{enable disable set-key}	- Enter enable to enable encryption for config file transfers. - Enter disable to disables encryption for config file transfers. - Enter set-key to configures the encryption key for config file transfers.
	<i>key</i>	Encryption key for config file transfers.

Defaults	None.

Examples	> transfer encrypt enable

Related Commands	clear transfer transfer download datatype transfer download filename transfer download mode transfer download path transfer download serverip transfer upload datatype transfer download filename transfer download mode transfer download path transfer download serverip transfer download start

transfer upload datatype

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

transfer upload datatype [**config** | **crashfile** | **errorlog** | **pac** | **radio-core-dump** | **signature** | **systemtrace** | **traplog**]

Syntax Description	
config	(Optional) Specifies the upload is a system configuration file.
crashfile	(Optional) Specifies the upload is a system crashfile
errorlog	(Optional) Specifies the upload is a system error log file
pac	(Optional) Specifies the upload is a system PAC file.
radio-core-dump	(Optional) Specifies the upload is a system radio error log file.
signature	(Optional) Specifies the upload is a system signature file.
systemtrace	(Optional) Specifies the upload is a system trace file.
traplog	(Optional) Specifies the upload is a system trap file.

Defaults This command has no defaults.

Command History	Release	Modification
	4.1	This command was revised to include the pac option.

Examples
 > **transfer upload datatype errorlog**

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 filename

To upload a specific file, use the **transfer upload filename** command.

transfer upload filename *filename*

Syntax Description

transfer	Transfer a file to or from the switch.
upload	Transfer a file from the switch.
filename	Set the FTP or TFTP filename.
<i>filename</i>	File name up to 16 alphanumeric characters.

Defaults

None.

Examples

```
> transfer upload filename build603
```

Related Commands

clear transfer
transfer 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 mode

To configure the transfer mode, use the **transfer upload mode** command.

transfer upload mode {ftp | tftp}

Syntax	Description
transfer	Transfer a file to or from the switch.
upload	Transfer a file from the switch.
mode	Set transfer mode.
ftp	Set the transfer mode to FTP.
tftp	Set the transfer mode to TFTP.

Defaults None.

Examples `> transfer upload mode tftp`

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 pac

To load a protected access credential (PAC) to support the local authentication feature and allow a client to import the PAC, use the **transfer upload pac** command. The client upload process uses a TFTP or FTP server.

transfer upload pac *username validity password*

Syntax Description

<i>username</i>	Specifies the user identity of the PAC.
<i>validity</i>	Specifies the validity period(days) of the PAC.
<i>password</i>	Specifies the password to protect the PAC.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> transfer upload datatype pac
> transfer upload pac user1 53 pass01
> transfer upload filename uploaded.pac
> transfer upload start
Mode ..... TFTP
TFTP Server IP ..... 10.0.24.21
TFTP Server Path ..... /client/
TFTP Filename ..... uploaded.pac
Data Type ..... PAC
PAC User ..... user1
PAC Validity ..... 53 days
PAC Password ..... pass01
Are you sure you want to start ? (Y/N) y
PAC transfer starting.
File transfer operation completed successfully.
```

Related Commands

clear transfer
transfer 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 password

To set the password for FTP transfer, use the **transfer upload password** command.

transfer upload password *password*

Syntax Description	transfer	Transfer a file to or from the switch.
	upload	Transfer a file from the switch.
	password	Set FTP password.
	<i>password</i>	Password.

Defaults	None.

Examples	<pre>>transfer upload password pass01</pre>

Related Commands	transfer upload mode transfer upload port transfer upload username

transfer upload path

To set a specific upload path, use the **transfer upload path** command.

transfer upload path *path*

Syntax Description	transfer	Transfer a file to or from the switch.
	upload	Transfer a file from the switch.
	path	Set TFTP or FTP Path.
	<i>path</i>	Directory path.

Defaults None.

Examples
 > transfer upload path c:\install\version2

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 port

To specify the FTP port, use the **transfer upload port** command

transfer upload port *port*

Syntax Description

transfer	Transfer a file to or from the switch.
upload	Transfer a file from the switch.
port	FTP port.
<i>port</i>	Set FTP port.

Defaults

The default FTP *port* is **21**.

Examples

```
>transfer upload port 23
```

Related Commands

[transfer upload mode](#)
[transfer upload password](#)
[transfer upload username](#)

transfer upload serverip

To configure the IP address of the TFTP server to upload files to, use the **transfer upload serverip** command.

transfer upload serverip *ip_address*

Syntax Description	transfer	Transfer a file to or from the switch.
	upload	Transfer a file from the switch.
	serverip	Enter IP address of the server.
	<i>ip_address</i>	Server IP address.

Defaults None.

Examples
 > **transfer upload serverip 175.34.56.78**

Related Commands

- clear transfer
- transfer 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 start

To initiate an upload, use the **transfer upload start** command.

transfer upload start

Syntax Description

transfer	Transfer a file to or from the switch.
upload	Transfer a file from the switch.
start	Initiate upload.

Defaults

None.

Examples

```
> transfer upload start
```

```
Mode..... TFTP
TFTP Server IP..... 172.16.16.78
TFTP Path..... c:\find\off/
TFTP Filename..... wps_2_0_75_0.aes
Data Type..... Code
```

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

```
Transfer Cancelled
```

Related Commands

clear transfer

transfer 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 username

To specify the FTP username, use the **transfer upload username** command.

transfer download username *username*

Syntax Description	transfer	Transfer a file to or from the switch.
	upload	Transfer a file from the switch.
	username	FTP username.
	<i>username</i>	Username.

Defaults None.

Examples `>transfer upload username ftp_username`

Related Commands

- [transfer upload mode](#)
- [transfer upload password](#)
- [transfer upload port](#)

Troubleshooting Commands

Use the **debug** commands to manage system debugging.



Caution

Debug commands are reserved for use only under direction of Cisco personnel. Please do not use these commands without direction from Cisco-certified staff.



Note

Enabling all **debug** commands on a system with many clients authenticating may result in some debugs being lost.

debug aaa

To configure AAA debug options, use the **debug aaa** command:

```
debug aaa { [all | detail | events | packet | ldap | local-auth | tacacs ] [ enable | disable]}
```

Syntax Description

all	Specifies debugging of all AAA messages.
detail	Specifies debugging of AAA errors.
events	Specifies debugging of AAA events.
packet	Specifies debugging of AAA packets.
ldap	Specifies debugging of the AAA LDAP events.
local-auth	Specifies debugging of the AAA local EAP events.
tacacs	Specifies debugging of the AAA TACACS+ events.
enable	Starts the debugging feature.
disable	Stops the debugging feature.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
> debug aaa ldap enable
```

Related Commands

```
debug aaa local-auth eap  
show running-config
```

debug aaa local-auth

To debug AAA local authentication on the controller, use the **debug aaa local-auth** command:

```
debug aaa local-auth {
  db [enable | disable] |
  eap [framework | method] [all | errors | events | packets | sm] [enable | disable] |
  shim [enable | disable]}
```

Syntax Description		
db		Configures debugging of the AAA local authentication backend messages and events.
eap		Configures debugging of the AAA local EAP authentication.
shim		Configures debugging of the AAA local authentication shim layer events.
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 This command has no defaults.

Command History	Release	Modification
	4.1	This command was introduced.

Examples
 > debug aaa local-auth eap method all enable

Related Commands
 show local-auth config
 show wlan

debug airewave-director

To configure the Airewave Director Software debug options, use the **debug airewave-director** command.

```
debug airewave-director { all | channel | detail | error | group | manager | message | packet |
                        power | profile | radar | rf-change } { enable | disable }
```

Syntax Description

debug	Debug parameters.
airewave-director	Airewave Director parameters.
{ all channel detail error group manager message packet power profile radar rf-change }	- Enter all to configure debug of all Airewave Director logs. - Enter channel to configure debug of Airewave Director channel assignment protocol - Enter detail to configure debug of Airewave Director detail logs. - Enter error to configure debug of Airewave Director error logs. - Enter group to configure debug of Airewave Director grouping protocol. - Enter manager to configure debug of Airewave Director manager. - Enter message to configure debug of Airewave Director messages. - Enter packet to configure debug of Airewave Director packets. - Enter power to configure debug of Airewave Director power assignment protocol and coverage hole detection. - Enter profile to configure debug of Airewave Director profile events. - Enter radar to configure debug of Airewave Director radar detection/avoidance protocol. - Enter rf-change to configure debug of Airewave Director rf changes.
{ enable disable }	- Enter enable to enable Airewave Director debug setting. - Enter disable to disable Airewave Director debug setting.

Defaults

None.

Examples

```
> debug airewave-director profile enable
> debug airewave-director profile disable
```

Related Commands

```
show sysinfo
debug disable-all
```

debug ap

To enable or disable remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use this command:

debug ap {enable | disable | command *cmd*} *Cisco_AP*

Syntax Description		
debug		Debug parameters.
ap		Debug lightweight access point parameters.
enable disable		Enable or disable debugging on a lightweight access point.
	Note	The debugging information is displayed only to the controller console and does not send output to a controller TELNET/SSH CLI session.
command		Specifies that a CLI command follows to be executed on the access point.
<i>cmd</i>		Command to be executed.
	Note	The command to be executed must be enclosed in double quotes, such as debug ap command "led flash 30" AP03 .
	Note	The output of the command displays only to the controller console and does not send output to a controller TELNET/SSH CLI session.
<i>Cisco_AP</i>		Name of a Cisco lightweight access point.

Defaults

Disabled.

Examples

To enable remote debugging on access point AP01:

```
> debug ap enable AP01
```

To execute the **config ap location** command on access point AP02:

```
> debug ap command "config ap location "Building 1" AP02"
```

To execute the flash LED command on access point AP03:

```
> debug ap command "led flash 30" AP03
```

Related Commands

show sysinfo
config sysname

debug ap enable

To enable or disable remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use this command:

debug ap {enable | disable | command *cmd*} *Cisco_AP*

Syntax Description	enable	Enables remote debugging.
	Note	The debugging information is displayed only to the controller console and does not send output to a controller TELNET/SSH CLI session.
	disable	Disables remote debugging.
	command	Specifies that a CLI command follows to be executed on the access point.
	<i>cmd</i>	Command to be executed.
	Note	The command to be executed must be enclosed in double quotes, such as debug ap command "led flash 30" AP03 .
	Note	The output of the command displays only to the controller console and does not send output to a controller TELNET/SSH CLI session.
	<i>Cisco_AP</i>	Cisco lightweight access point name.

Defaults

None.

Examples

To enable remote debugging on access point AP01:

```
> debug ap enable AP01
```

To disable remote debugging on access point AP02:

```
> debug ap disable AP02
```

To execute the flash LED command on access point AP03:

```
> debug ap command "led flash 30" AP03
```

Related Commands

show sysinfo
config sysname

debug arp

To configure ARP debug options, use the **debug arp** command.

debug arp {all | detail | events | message} {enable | disable}

Syntax Description	debug	Debug parameters.
	arp	ARP parameters.
	{all detail error message}	- Enter all to configure debug of all arp logs. - Enter detail to configure debug of arp detail messages.. - Enter error to configure debug of arp errors. - Enter message to configure debug of arp messages.
	{enable disable}	- Enter enable to enable arp debug setting. - Enter disable to disable arp debug setting.

Defaults None.

Examples

```
> debug arp error enable
> debug arp error disable
```

Related Commands

show sysinfo
debug disable-all

debug bcast

To configure debug of broadcast options, use the **debug bcast** command.

```
debug bcast {all | error | message | igmp | detail} {enable | disable}
```

Syntax Description	debug	Debug parameters.
	bcast	bcast parameters.
	all error message igmp detail	- Enter all to configure debug of all broadcast logs. - Enter detail to configure debug of broadcast detailed messages. - Enter error to configure debug of broadcast errors. - Enter igmp to configure debug of broadcast messages. - Enter message to configure debug of broadcast messages.
	{enable disable}	- Enter enable to enable broadcast debug setting. - Enter disable to disable broadcast debug setting.

Defaults	None.

Examples	<pre>> debug bcast message enable > debug bcast message disable</pre>

Related Commands	<pre>show sysinfo debug disable-all</pre>

debug cac

To configure call admission control (CAC) debug options, use the **debug cac** command.

debug cac {all | event | packet} {enable | disable}

Syntax Description	debug	Debug parameters.
	cac	Debug call admission control parameters.
	all event packet	- Enter all to configure debugging options for all CAC messages. - Enter event to configure debugging options for CAC events. - Enter packet to configure debugging options for selected CAC packets.
	enable disable	- Enter enable to enable debug setting. - Enter disable to disable debug setting.

Defaults Disabled.

Examples

```
> debug cac event enable
> debug cac event disable
```

Related Commands

```
config {802.11a | 802.11b} cac video acm
config {802.11a | 802.11b} {enable | disable} network
config {802.11a | 802.11b} cac video max-bandwidth
config {802.11a | 802.11b} cac video roam-bandwidth
config {802.11a | 802.11b} cac video tspec-inactivity-timeout
config {802.11a | 802.11b} cac voice acm
config {802.11a | 802.11b} cac voice load-based
config {802.11a | 802.11b} cac voice max-bandwidth
config {802.11a | 802.11b} cac voice roam-bandwidth
config {802.11a | 802.11b} cac voice stream-size
config {802.11a | 802.11b} cac voice tspec-inactivity-timeout
```

debug crypto

To configure hardware cryptographic debug options, use the **debug crypto** command.

```
debug crypto {all | sessions | trace | warning} {enable | disable}
```

Syntax Description	debug	Debug parameters.
	dhcp	DHCP parameters.
	{all sessions trace warning}	- Enter all to configure debug of all hardware crypto messages. - Enter sessions to configure debug of hardware crypto sessions. - Enter trace to configure debug of hardware crypto sessions. - Enter warning to configure debug of hardware crypto sessions.
	{enable disable}	- Enter enable to enable debug setting. - Enter disable to disable debug setting.

Defaults
None.

Examples
> debug sessions enable
> debug sessions disable

Related Commands
show sysinfo
debug disable-all

debug dhcp

To configure DHCP debug options, use the **debug dhcp** command.

debug dhcp {message | packet} {enable | disable}

Syntax Description	debug	Debug parameters.
	dhcp	DHCP parameters.
	{message packet}	- Enter message to configure debug of DHCP error messages. - Enter packet to configure debug of DHCP packets.
	{enable disable}	- Enter enable to enable DHCP debug setting. - Enter disable to disable DHCP debug setting.

Defaults None.

Examples

```
> debug dhcp message enable
> debug dhcp message disable
```

Related Commands debug disable-all

debug disable-all

To disable all debug messages, use the **debug disable-all** command.

debug disable-all

Syntax Description	debug	Debug parameters.
	disable-all	Disables all debug messages.

Defaults	Disabled.

Examples	> debug disable-all

Related Commands	debug aaa
	debug airewave-director
	debug arp
	debug bcast
	debug crypto
	debug dhcp
	debug dot11
	debug dot1x
	debug l2age
	debug lwapp
	debug mac
	debug mobility
	debug nac
	debug ntp
	debug pem
	debug pm
	debug poe
	debug rbc
	debug snmp
	debug transfer
	debug wcp
	debug wps

debug dot11

To configure dot11 events debug options, use the **debug dot11** command.

```
debug dot11 {all | load-balancing | management | mobile | rfid | rldp | rogue | state} {enable | disable}
```

Syntax Description	debug	Debug parameters.
	dot11	dot11 events parameters.
	{all load-balancing management mobile rfid rldp rogue state}	- Enter all to configure debug of all 802.11 messages. - Enter load-balancing to configure debug of 802.11 load balancing events. - Enter management to configure debug of 802.11 MAC management messages. - Enter mobile to configure debug of 802.11 mobile events. - Enter rfid to configure debug of 802.11 RFID tag module. - Enter rldp to configure debug of 802.11 Rogue Location Discovery. - Enter rogue to configure debug of 802.11 rogue events. - Enter state to configure debug of 802.11 mobile state transitions.
	{enable disable}	- Enter enable to enable dot11 debug setting. - Enter disable to disable dot11 debug setting.

Defaults None.

Examples

```
> debug dot11 state enable
> debug dot11 state disable
```

Related Commands debug disable-all

debug dot11 mgmt interface

To view 802.11 management interface events, use the **debug dot11 mgmt interface** command.

debug dot11 mgmt interface

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples

> debug dot11 mgmt interface

Related Commands

debug disable-all

debug dot11 mgmt msg

To view 802.11 management messages, use the **debug dot11 mgmt msg** command.

debug dot11 mgmt msg

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples	> debug dot11 mgmt msg

Related Commands	debug disable-all

debug dot11 mgmt ssid

To view 802.11 SSID management events, use the **debug dot11 mgmt ssid** command.

debug dot11 mgmt ssid

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples	> debug dot11 mgmt ssid

Related Commands	debug disable-all

debug dot11 mgmt state-machine

To view 802.11 state machine, use the **debug dot11 mgmt state-machine** command.

debug dot11 mgmt state-machine

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples	> debug dot11 mgmt state-machine

Related Commands	debug disable-all

debug dot11 mgmt station

To view client events, use the **debug dot11 mgmt station** command.

debug dot11 mgmt station

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples	> debug dot11 mgmt station

Related Commands	debug disable-all

debug dot1x

To configure dot1x debug options, use the **debug dot1x** command.

debug dot1x {aaa | all | events | packet | states} {enable | disable}

Syntax Description	debug	Debug parameters.
	dot1x	dot1x parameters.
	{aaa all events packet states}	- Enter aaa to configure debug of 802.1X AAA interactions. - Enter all to configure debug of all 802.1x messages. - Enter events to configure debug of 802.1x 802.1X events. - Enter packet to configure debug of 802.1x 802.1X packets. - Enter states to configure debug of 802.1x mobile state transitions.
	{enable disable}	- Enter enable to enable dot1x debug setting. - Enter disable to disable dot1x debug setting.

Defaults None.

Examples

```
> debug dot1x state enable
> debug dot1x state disable
```

Related Commands

```
debug disable-all
debug dot11
```

debug l2age

To configure debug of Layer 2 Age timeout messages, use the **debug l2age** command.

```
debug l2age {enable | disable}
```

Syntax Description	debug	Debug parameters.
	l2age	Layer 2 Age Timeout Messages.
	{enable disable}	- Enter enable to enable l2age debug setting. - Enter disable to disable l2age debug setting.

Defaults None.

Examples > debug l2age enable
 > debug l2age disable

Related Commands debug disable-all

debug lwapp

To configure LWAPP debug options, use the **debug lwapp** command. This is a helpful command to debug when an AP does not join a controller.

debug lwapp {detail | error | events | packet} {enable | disable}

Syntax Description	debug	Debug parameters.
	lwapp	lwapp parameters.
	{detail error events packet}	- Enter detail to configure debug of LWAPP detail. - Enter error to configure debug of LWAPP errors. - Enter events to configure debug of LWAPP events and errors. - Enter packet to configure debug of LWAPP packet trace.
	{enable disable}	- Enter enable to enable lwapp debug setting. - Enter disable to disable lwapp debug setting.
Defaults	None.	
Examples	<pre>> debug lwapp packet enable > debug lwapp packet disable</pre>	
Related Commands	debug disable-all	

debug lwapp console cli

To begin debugging of the access point console CLI, use the **debug lwapp console cli** command from the access point console port.

debug lwapp console cli

**Note**

This access point CLI command must be issued from the access point console port.

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no defaults.

Command History

Release	Modification
4.1	This command was introduced.

Examples

```
AP# debug lwapp console cli
LWAPP console CLI allow/disallow debugging is on
```

Related Commands

lwapp ap controller ip address
clear lwapp private-config

debug lwapp reap

To obtain debug information regarding general hybrid-REAP activities, use the **debug lwapp reap** command.

debug lwapp reap

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no defaults.

Command History

Release	Modification
4.2	This command was introduced.

Examples

```
> debug lwapp reap
```

Related Commands

debug lwapp reap mgmt
debug lwapp reap load
debug dot11 mgmt interface
debug dot11 mgmt msg
debug dot11 mgmt ssid
debug dot11 mgmt state-machine
debug dot11 mgmt station

debug lwapp reap load

To view payload activities, use the **debug lwapp reap load** command.

debug lwapp reap load



Note Viewing payload activities is useful when the hybrid-REAP access point boots up in standalone mode.

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples > debug lwapp reap load

Related Commands

- debug lwapp reap
- debug lwapp reap mgmt
- debug dot11 mgmt interface

debug lwapp reap mgmt

To view client authentication and association messages, use the **debug lwapp reap mgmt** command.

debug lwapp reap mgmt

Syntax Description	This command has no arguments or keywords.

Defaults	This command has no defaults.

Command History	Release	Modification
	4.2	This command was introduced.

Examples	> debug lwapp reap mgmt

Related Commands	debug lwapp reap debug lwapp reap load

debug mac

To configure MAC debugging, use the **debug mac** command.

```
debug mac {disable | addr MAC}
```

Syntax Description	debug	Debug parameters.
	mac	MAC address parameters.
	disable	Enter disable to disable MAC debugging.
	addr	Enter addr to configure the MAC address.
	MAC	MAC address.

Defaults	None.

Examples	> debug mac addr 00.oc.41.07.33.a6 > debug mac disable

Related Commands	debug disable-all

debug mobility

To troubleshoot mobility issues, use the **debug mobility** command.

debug mobility handoff {enable | disable}—Debugs mobility handoff issues.

debug mobility keep-alive {enable | disable} all—Dumps the keepalive packets for all mobility anchors.

debug mobility keep-alive {enable | disable} *IP_address*—Dumps the keepalive packets for a specific mobility anchor.

debug mobility multicast {enable | disable}— Enables or disables debugging of multicast usage for mobility messages.

Syntax Description

enable	Starts debugging of the feature.
disable	Stops debugging of the feature.
handoff	Begins debugging mobility packets.
keep-alive	Begins debugging of mobility keepalive messages.
multicast	Begins debugging of multicast usage

Defaults

This command has no defaults.

Examples

```
> debug mobility handoff enable
> debug mobility keep-alive disable all
> debug mobility keep-alive enable 172.19.28.40
> debug mobility multicast enable
```

Related Commands

debug disable-all
show mobility summary

debug nac

To configure debug of Network Access Control (NAC), use the **debug nac** command.

```
debug nac { events | packet } { enable | disable }
```

Syntax Description	debug	Debug parameters.
	nac	Network Access Control (NAC) parameters.
	{ events packet }	- Enter events to configure debug of NAC events. - Enter packet to configure debug of NAC packets.
	{ enable disable }	- Enter enable to enable NAC debug setting. - Enter disable to disable NAC debug setting.

Defaults	None.

Examples	<pre>> debug nac events enable > debug nac events disable</pre>

Related Commands	debug disable-all

debug ntp

To configure debug of Network Time Protocol (NTP), use the **debug ntp** command.

debug ntp {**detail** | **low** | **packet**} {**enable** | **disable**}

Syntax Description	debug	Debug parameters.
	ntp	Network Time Protocol (NTP) parameters.
	{ detail low packet }	- Enter detail to configure debug of detailed NTP messages. - Enter low to configure debug of NTP messages. - Enter packet to configure debug of NTP packets.
	{ enable disable }	- Enter enable to enable NTP debug setting. - Enter disable to disable NTP debug setting.

Defaults None.

Examples

```
> debug ntp packet enable
> debug ntp packet disable
```

Related Commands debug disable-all

debug pem

To configure the access policy manager debug options, use the **debug pem** command.

```
debug pem {events | state} {enable | disable}
```

Syntax Description	debug	Debug parameters.
	pem	Access policy manager debug options.
	{events state}	- Enter packet to configure debug of policy manager events.. - Enter events to configure debug of policy manager State Machine.
	{enable disable}	- Enter enable to enable access policy manager debug setting. - Enter disable to disable access policy manager debug setting.

Defaults	None.

Examples	> debug pem state enable > debug pem state disable

Related Commands	debug disable-all

debug pm

To configure debug of security policy manager module, use the **debug pm** command.

debug pm all disable

```
debug pm {config | hwcrypto | ikemsg | init | list | message | pki | rng | rules | sa-export |
sa-import | ssh-l2tp | ssh-appgw | ssh-engine | ssh-int | ssh-pmgr | ssh-ppp | ssh-tcp} {enable
| disable}
```

Syntax Description	debug	Debug parameters.
	pm	Security policy manager module parameters.
	all disable	Used to disable all debugging in the policy manager module.
	{ config hwcrypto ikemsg init list message pki rng rules sa-export sa-import ssh-l2tp ssh-appgw ssh-engine ssh-int ssh-pmgr ssh-ppp ssh-tcp }	- Enter config to configure debug of policy manager configuration. - Enter hwcrypto to configure debug of hardware offload events. - Enter ikemsg to configure debug of IKE messages. - Enter init to configure debug of policy manager initialization events. - Enter list to configure debug of policy manager list mgmt. - Enter message to configure debug of policy manager message queue events. - Enter pki to configure debug of PKI-related events. - Enter rng to configure debug of random number generation. - Enter rules to configure debug of layer 3 policy events. - Enter sa-export to configure debug of SA export (mobility). - Enter sa-import to configure debug of SA import (mobility). - Enter ssh-l2tp to configure debug of policy manager l2tp handling. - Enter ssh-appgw to configure debug of application gateways. - Enter ssh-engine to configure debug of the policy manager engine. - Enter ssh-int to configure debug of the policy manager interceptor. - Enter ssh-pmgr to configure debug of the policy manager policy mgr. - Enter ssh-ppp to configure debug of policy manager ppp handling. - Enter ssh-tcp to configure debug of policy manager tcp handling.
	{ enable disable }	- Enter enable to enable mobility debug setting. - Enter disable to disable mobility debug setting.

Defaults

None.

Examples

```
> debug pm ssh-pmgr enable
> debug pm ssh-pmgr disable
```

Related Commands debug disable-all

debug poe

To configure debug of Power over ethernet debug options, use the **debug poe** command.

debug poe {**detail** | **error** | **message**} {**enable** | **disable**}

Syntax Description	debug	Debug parameters.
	poe	Power over ethernet debug options parameters.
	{ detail error message }	- Enter detail to configure debug of POE detail logs. - Enter error to configure debug of POE error logs. - Enter message to configure debug of POE messages.
	{ enable disable }	- Enter enable to enable POE debug setting. - Enter disable to disable POE debug setting.

Defaults None.

Examples

```
> debug poe message enable
> debug poe message disable
```

Related Commands debug disable-all

debug rbc

To configure Router Blade Control (RBC) debug options, use the **debug rbc** command.

```
debug rbc {all | detail | errors | packet} {enable | disable}
```

Syntax Description	debug	Debug parameters.
	rbc	RBC parameters.
	{all detail errors packet}	- Enter all to configure debug of RBC. - Enter detail to configure debug of RBC detail. - Enter errors to configure debug of RBC errors. - Enter packet to configure debug of RBC packet trace.
	{enable disable}	- Enter enable to enable RBC debug setting. - Enter disable to disable RBC debug setting.

Defaults	None.

Examples	> debug rbc packet enable > debug rbc packet disable

Related Commands	debug disable-all

debug rfid

To configure radio-frequency identification (RFID) debug options, use the **debug rfid** command.

debug rfid { **all** | **detail** | **errors** | **nmosp** | **receive** } { **enable** | **disable** }

Syntax Description	debug	Debug parameters.
	rbcp	RBCP parameters.
	{ all detail errors nmosp receive }	- Enter all to configure debug of all RFID messages. - Enter detail to configure debug of RFID detail. - Enter errors to configure debug of RFID error messages. - Enter nmosp to configure debug of RFID Network Mobility Services Protocol (NMSP) messages. - Enter receive to configure debug of incoming RFID tag messages.
	{ enable disable }	- Enter enable to enable RFID debug setting. - Enter disable to disable RFID debug setting.

Defaults None.

Examples

```
> debug rfid errors enable
> debug rfid errors disable
```

Related Commands debug disable-all

debug snmp

To configure SNMP debug options, use the **debug snmp** command.

```
debug snmp {agent | all | mib | trap} {enable | disable}
```

Syntax Description	debug	Debug parameters.
	snmp	lwapp parameters.
	{agent all mib trap}	- Enter agent to configure debug of SNMP agent. - Enter all to configure debug of all SNMP messages. - Enter mib to configure debug of SNMP MIB. - Enter trap to configure debug of SNMP traps.
	{enable disable}	- Enter enable to enable SNMP debug setting. - Enter disable to disable SNMP debug setting.

Defaults	None.

Examples	> debug snmp trap enable > debug snmp trap disable

Related Commands	debug disable-all

debug transfer

To configure transfer debug options, use the **debug transfer** command.

debug transfer { **all** | **tftp** | **trace** } { **enable** | **disable** }

Syntax Description	debug	Debug parameters.
	transfer	transfer parameters.
	{ all tftp trace }	- Enter all to configure debug of all transfer messages. - Enter tftp to configure debug of tftp transfers. - Enter trace to configure debug of transfer/upgrade.
	{ enable disable }	- Enter enable to enable transfer debug setting. - Enter disable to disable transfer debug setting.
Defaults	None.	
Examples	<pre>> debug transfer trace enable > debug transfer trace disable</pre>	
Related Commands	debug disable-all	

debug wcp

To configure wcp debug options, use the **debug wcp** command.

debug wcp {events | packet} {enable | disable}

Syntax Description	debug	Debug parameters.
	wcp	wcp parameters.
	{events packet}	- Enter events to configure debug of WLAN Control Protocol (WCP) Events. - Enter packet to configure debug of WLAN Control Protocol (WCP) Packets.
	{enable disable}	- Enter enable to enable wcp debug setting. - Enter disable to disable wcp debug setting.

Defaults	None.

Examples	<pre>> debug wcp packet enable > debug wcp packet disable</pre>

Related Commands	debug disable-all

debug wps

To configure wps debug options, use the **debug wps** command.

config wps sig {enable | disable}

Syntax Description	debug	debug parameters.
	wps	WPS parameters.
	sig	Signature parameters.
	{enable disable}	- Enter enable to enable wps debug setting. - Enter disable to disable wps debug setting.

Defaults	None.

Examples	<pre>> debug wps sig enable > debug wps sig disable</pre>

Related Commands	debug disable-all

eping

To test mobility Ethernet over IP (EoIP) data packet communication between two controllers, use the **eping** command.

eping *mobility_peer_IP_address*

Syntax Description

eping	Initiate a ping request and reply message for EoIP mobility packets.
<i>mobility_peer_IP_address</i>	The IP address of a controller that belongs to a mobility group.

Defaults

None.

Usage Guidelines

This command tests the mobility data traffic over the management interface.



Note This ping test is not Internet Control Message Protocol (ICMP) based. The term “ping” is used to indicate an echo request and an echo reply message.

Examples

> **eping** 172.12.35.31

Related Commands

- mping**
- config logging buffered debugging**
- show logging**
- debug mobility handoff enable**

mping

To test mobility UDP control packet communication between two controllers, use the **mping** command.

mping *mobility_peer_IP_address*

Syntax Description	
mping	Initiate a ping request and reply message for UDP mobility packets.
<i>mobility_peer_IP_address</i>	The IP address of a controller that belongs to a mobility group.

Defaults None.

Usage Guidelines This test runs over mobility UDP port 16666. It tests whether the mobility control packet can be reached over the management interface.



Note This ping test is not Internet Control Message Protocol (ICMP) based. The term “ping” is used to indicate an echo request and an echo reply message.

Examples > **mping** 172.12.35.31

Related Commands

- eping**
- config logging buffered debugging**
- show logging**
- debug mobility handoff enable**

