Cisco Wireless LAN Controller Command Reference

Release 3.1.64.0
August 22, 2005

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-7427-02

Cisco Wireless LAN Controller Command Reference

Cisco Wireless LAN Controller Command Reference

The Cisco Wireless LAN Solution command line interface (CLI) allows operators to connect an ASCII console to the Cisco Wireless LAN controller and configure the Cisco Wireless LAN controller and its associated Cisco 1000 Series lightweight access points using the command line interface.

Note See the related product guide for a description of the most important CLI tasks.

? command

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

?

(command name) ?

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

Examples

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

```
> ?

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

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

```
> transfer download d?

datatype
```

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

```
> transfer download datatype ?

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

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
```

Viewing Configurations

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

show 802.11a

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

show 802.11a

Syntax Description

show	Display configurations.
802.11a	802.11a configurations.

Defaults

None.

Examples

```
> show 802.11a

802.11a Network.............................. 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
Beacon Interval.............................. 100
CF Pollable mandatory........................ Disabled
CF Poll Request mandatory.................... Disabled
CFP Period................................... 4
CFP Maximum Duration......................... 100
Default Channel.............................. 36
Default Tx Power Level....................... 1
DTIM Period.................................. 10
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
RTS Threshold................................ 2347
Short Retry Limit............................ 7
TI Threshold................................. -50
```

Related Commands

show 802.11b, **show advanced 802.11a channel**, **show advanced 802.11a group**, **show advanced 802.11a logging**, **show advanced 802.11a monitor**, **show advanced 802.11a power**, **show advanced 802.11a profile**, **show advanced 802.11a summary**

show 802.11b

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

show 802.11b

Syntax Description

show	Display configurations.
802.11b	802.11b/g configurations.

Defaults

None.

Examples

```
> show 802.11b

802.11b Network.................................. Enabled
11gSupport....................................... Enabled
802.11b/g Operational Rates
    802.11b/g 1M Rate............................ Mandatory
    802.11b/g 2M Rate............................ Mandatory
    802.11b/g 5.5M Rate.......................... Mandatory
    802.11b/g 11M Rate........................... Mandatory
    802.11g 6M Rate.............................. Supported
    802.11g 9M Rate.............................. Supported
    802.11g 12M Rate............................. Supported
    802.11g 18M Rate............................. Supported
    802.11g 24M Rate............................. Supported
    802.11g 36M Rate............................. Supported
    802.11g 48M Rate............................. Supported
    802.11g 54M Rate............................. Supported
Beacon Interval.................................. 100
CF Pollable mode................................. Disabled
CF Poll Request mandatory........................ Disabled
CFP Period....................................... 4
CFP Maximum Duration............................. 60
Default Channel.................................. 1
Default Tx Power Level........................... 1
DTPC  Status..................................... Enabled
Call Admission Limit  ........................... 105
G711 CU Quantum ................................. 15
DTIM Period...................................... 1
ED Threshold..................................... -50
Fragmentation Threshold.......................... 2346
Long Retry Limit................................. 4
Maximum Rx Life Time............................. 512
Max Tx MSDU Life Time............................ 512
Medium Occupancy Limit........................... 100
PBCC mandatory................................... Disabled
Pico-Cell Status................................. Disabled
RTS Threshold.................................... 2347
Short Preamble mandatory......................... Enabled
Short Retry Limit................................ 7
```

Related Commands **show 802.11a**, **show advanced 802.11b channel**, **show advanced 802.11b group**, **show advanced 802.11b logging**, **show advanced 802.11b monitor**, **show advanced 802.11b txpower**, **show advanced 802.11b profile**, **show advanced 802.11b summary**

show acl

To display system Access Control Lists (ACLs), use the **show acl** command.

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

Syntax Description

show acl	Command action.
{summary | detailed}	Display a summary of all ACLs or display the detailed information about a specific ACL.
acl_name	ACL name up to 32 alphanumeric characters.

Defaults

None.

Examples

```
> show acl summary

ACL Name                         Applied
-------------------------------- -------
Pubs Only                        Yes
Macnica                          Yes
```

Related Commands

config interface acl

SHOW ADVANCED 802.11A COMMANDS

Use the show advanced 802.11a commands to display advanced 802.11a configuration 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	Display 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..................... AUTO
  Channel Update Interval..................... 600 seconds
  Channel Update Contribution................. SNI.
  Channel Assignment Leader................... 00:0b:85:02:0d:20
  Last Run.................................... 374 seconds ago
  Channel Energy Levels
    Minimum................................... -84 dBm
    Average................................... -84 dBm
    Maximum................................... -84 dBm
  Channel Dwell Times
    Minimum................................... 0 days, 19 h 07 m 57 s
    Average................................... 0 days, 19 h 08 m 29 s
    Maximum................................... 0 days, 19 h 09 m 11 s
```

Related Commands

config 802.11a channel

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	Display 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................................... a5:6b:ac:10:01:6b
    802.11a Group Member................................. a5:6b:ac:10:01:6b
  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	Display 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	Display 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 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	Display 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
  RxAbort : Raw Power Drop Status....................... Disabled
  RxAbort : Raw Power Drop Threshold.................... 10
  RxAbort : Low RSSI Status............................. Disabled
  RxAbort : Low RSSI Threshold.......................... 0
  RxAbort : Wrong BSSID Status.......................... Disabled
  RxAbort : Wrong 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 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	Display 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................ a5:6b:ac:10:01:6b
  Last Run........................................ 384 seconds ago
```

Related Commands

config advanced 802.11a txpower-update, **config 802.11a txPower**

show advanced 802.11a profile

To display the advanced 802.11a Cisco 1000 Series lightweight access point performance profiles, use the **show advanced 802.11a profile** command.

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

Syntax Description

show	Display configurations.
advanced	Advanced parameters.
802.11a	802.11a network.
profile	Cisco Radio performance profile.
global	All Cisco 1000 Series lightweight access points.
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

None.

Examples

```
> show advanced 802.11a profile global

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

> show advanced 802.11a profile AP1

Cisco 1000 Series lightweight access point performance profile not customized
```

This response indicates that the performance profile for this Cisco 1000 Series 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 coverage**, **config advanced 802.11b profile customize**, **config advanced 802.11b profile exception**, **config advanced 802.11b profile foreign**, **config advanced 802.11b profile level**, **config advanced 802.11b profile noise**, **config advanced 802.11b profile throughput**, **config advanced 802.11b profile utilization**

show advanced 802.11a summary

To display the advanced 802.11a Cisco 1000 Series 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	Display configurations.
advanced	Advanced parameters.
802.11a	802.11a network.
summary	Cisco 1000 Series 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 Asterisks next to channel numbers or power levels indicate that they are being controlled by the global algorithm settings.

Related Commands

show advanced 802.11b summary

SHOW ADVANCED 802.11B COMMANDS

Use the show advanced 802.11b commands 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	Display 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..................... OFF
  Channel Update Interval..................... 600 seconds
  Channel Update Contribution................. SNI.
  Channel Assignment Leader................... 00:0b:85:02:0d:20
  Last Run.................................... 157 seconds ago
  Channel Energy Levels
    Minimum................................... unknown
    Average................................... unknown
    Maximum................................... unknown
  Channel Dwell Times
    Minimum................................... unknown
    Average................................... unknown
    Maximum................................... unknown
```

Related Commands

config 802.11b channel

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	Display 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............................  a5:6b:ac:10:01:6b
     802.11b Group Member..........................  a5:6b:ac:10:01:6b
   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	Display 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	Display 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 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	Display 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 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	Display configurations.
advanced	Advanced parameters.
802.11b	802.11b/g network.
profile	Cisco 1000 Series lightweight access point performance profile.
global	All Cisco 1000 Series lightweight access points.
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

None.

Examples

```
> show advanced 802.11b profile global

Default 802.11b Cell 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 1000 Series lightweight access point performance profile not customized
```

This response indicates that the performance profile for this Cisco 1000 Series 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 coverage**, **config advanced 802.11b profile customize**, **config advanced 802.11b profile exception**, **config advanced 802.11b profile foreign**, **config advanced 802.11b profile level**, **config advanced 802.11b profile noise**, **config advanced 802.11b profile throughput**, **config advanced 802.11b profile utilization**

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	Display 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............... 00:0b:85:02:0d:20
  Last Run....................................... 427 seconds ago
```

Related Commands

config 802.11b txPower

show advanced 802.11b summary

To display the advanced 802.11b/g Cisco 1000 Series 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	Display configurations.
advanced	Advanced parameters.
802.11b	802.11b/g network.
summary	Cisco 1000 Series 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 client-handoff

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

show advanced client-handoff

Syntax Description

show	Display 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 statistics

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

show advanced statistics

Syntax Description

show	Display 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	Display 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
EAP Request Timeout (seconds).................. 8
```

Related Commands

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

SHOW AP COMMANDS

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

show ap auto-rf

To display the auto-rf settings for a Cisco 1000 Series lightweight access point, use the **show ap auto-rf** command.

show ap auto-rf {802.11a | 802.11b} *Cisco_AP*

Syntax Description

show	Display configurations.
ap auto-rf	Cisco Radio.
{802.11a | 802.11b}	802.11a or 802.11b/g setting.
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

None.

Examples

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

Number Of Slots..................................... 2
Rad 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
  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 config

To display the detailed configuration for an 802.11b/g Cisco 1000 Series lightweight access point, use the **show ap config** command.

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

Syntax Description

show	Display configurations.
ap	Cisco Radio.
{802.11a | 802.11b | general}	802.11a, 802.11b/g or general settings.
Cisco_AP	Cisco 1000 Series 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 ......................................... Local
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 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  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 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
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
```

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

show ap core-dump

To display the memory core dump setting for a Cisco 1000 Series lightweight access point, use the **show ap core-dump** command.

show ap core-dump *Cisco_AP*

Syntax Description

show	Display configurations.
ap	Cisco Radio.
core-dump	Display the memory core dump setting for an access point.
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

None.

Examples

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

Related Commands

config ap stats-timer

show ap crash-file

To display the list of both crash and radio core dump files generated by Cisco 1000 Series lightweight access points, use the **show ap crash-file** command.

show ap crash-file

Syntax Description

show	Display configurations.
ap	Cisco Radio.
crash-file	Display the list of both crash and radio core dump files generated by access points. The generated information includes size and memory usage.

Defaults

None.

Examples

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

Related Commands

config ap stats-timer

show ap stats

To display the statistics for a Cisco 1000 Series lightweight access point, use the **show ap stats** command.

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

Syntax Description

show	Display configurations.
ap	Cisco Radio.
{802.11a | 802.11b}	802.11a or 802.11b/g statistics.
Cisco_AP	Cisco 1000 Series 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 stats-timer

show ap summary

To display a summary of all Cisco 1000 Series lightweight access points attached to the Cisco Wireless LAN controller, use the **show ap summary** command. A list containing each Cisco 1000 Series lightweight access point name, number of slots, manufacturer, MAC address, location and Cisco Wireless LAN controller port number is displayed.

show ap summary

Syntax Description

show	Display configurations.
ap	All Cisco 1000 Series lightweight access points.
summary	Summary of all Cisco 1000 Series lightweight access points.

Defaults

None.

Examples

```
> show ap summary

AP Name             Slots  AP Model             MAC Addr           Location          Port
------------------  -----  -------------------  -----------------  ----------------  -----
AP01                2      AIR-AP1210           00:0b:85:01:18:b0   default location  12
AP02                2      AIR-AP1210           00:0b:85:01:12:60   default location  11
```

Related Commands

show advanced 802.11a summary, **show advanced 802.11b summary**, **show certificate summary**, **show client summary**, **show mobility summary**, **show radius summary**, **show rogue-ap summary**, **show wlan 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	Display configurations.
ap	All Cisco 1000 Series lightweight access points.
wlan	Wireless LAN parameter.
{802.11a | 802.11b}	802.11a or 802.11b/g statistics.
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

None.

Examples

```
> show ap wlan 802.11a AP01

Cisco AP is not in override mode.
```

Related Commands

show advanced 802.11a summary, **show advanced 802.11b summary**, **show certificate summary**, **show client summary**, **show mobility summary**, **show radius summary**, **show rogue-ap summary**, **show wlan summary**

show arp switch

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

show arp switch

Syntax Description

show	Display 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
-------------------- ---------------- ------------
00:C0:A8:87:EA:78   172.19.1.158    service port    1
00:06:5B:3D:0B:5C   172.19.1.2      service port
00:D0:59:9D:5E:06   172.19.1.106    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	Display configurations.
auth-list	Display 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
-----------------------   ----------   ----------------------------------------
00:34:54:56:67:89         MIC
```

Related Commands

config auth-list

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	Display configurations.
exclusionist	Manual Exclusion List.

Defaults

None.

Examples

```
> show exclusionlist

MAC Address              Description
-----------------------  --------------------------------
00:50:08:00:00:f5        Disallowed Client
```

Related Commands

config exclusionlist add, **config exclusionlist delete**, **config exclusionlist description**, **show client**

show boot

Each Cisco Wireless LAN controller retains one primary and one backup OS 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	Display configurations.
boot	Software bootable versions.

Defaults

None.

Examples

```
> show boot

Primary Boot Image.............................. 2.0.133.0 (active)
Backup Boot Image.............................. 2.0.125.0
```

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	Display configurations.
certificate	All certificates.
compatibility	Compatibility of certificates.

Defaults

None.

Examples

```
> show certificate compatibility

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

Related Commands

show certificate summary

show certificate summary

To display a summary of all certificates active in the Cisco Wireless LAN controller, use the **show certificate summary** command.

show certificate summary

Syntax Description

show	Display configurations.
certificate	All certificates.
summary	Synopsis of all certificates.

Defaults

None.

Examples

```
> show certificate summary

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

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 1000 Series 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	Display configurations.
ap	Cisco Radio.
{802.11a | 802.11b}	802.11a or 802.11b/g clients.
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

None.

Examples

```
> show client ap 802.11b AP1

MAC Address        AP Id   Status         WLAN Id    Authenticated
-----------------  ------  -------------  ---------  -------------
00:0c:41:0a:33:13      1   Associated     1          No
```

Related Commands

show client detail, **show client summary**, **show client username**, **show exclusionlist**

show client detail

To display detailed information for a client on a Cisco 1000 Series 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*

Syntax Description

show	Display configurations.
client	802.11a or 802.11b/g client.
detail	Connectivity information.
MAC	MAC address of the specific client.

Defaults

None.

Examples

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

Client MAC Address.............................. 00:0c:41:07:33:a6
Client Username................................. N/A
AP MAC Address.................................. 00:0b:85:01:18:b0
Client State.................................... Associated
Wireless LAN Id................................. 1
IP Address...................................... Unknown
Association Id.................................. 1
Authentication Algorithm........................ Shared Key
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 0
Mirroring....................................... Disabled
QoS Level....................................... Gold
Diff Serv Code Point (DSPC)..................... disabled
802.1P Priority Tag............................. disabled
Mobility State.................................. Local
Mobility Move Count............................. 0
Security Policy Completed....................... No
Policy Manager State............................ DHCP_REQD
Policy Manager Rule Created..................... No
NPU Fast Notified............................... Yes
Policy Type..................................... N/A
Encryption Cipher............................... WEP (104 bits)
EAP Type........................................ Unknown
Interface....................................... management
VLAN............................................ 0
Client Capabilities:
      CF Pollable............................... Not implemented
      CF Poll Request........................... Not implemented
      Short Preamble............................ Not implemented
      PBCC...................................... Not implemented
      Channel Agility........................... Not implemented
```

```
      Listen Interval..............................  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 Policy Errors......................  0
      Radio Signal Strength Indicator.............  Unavailable
      Signal to Noise Ratio.......................  Unavailable
Nearby AP Statistics:
      AP03(slot 0) 24643 seconds ago..............  -11 dBm
```

Related Commands **show client ap**, **show client summary**, **show client username**, **show exclusionlist**

show client summary

To display a summary of clients associated with a Cisco 1000 Series 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	Display 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
-----------------  -----------------  -------------  ----  ----  --------  ----

00:01:24:60:16:9f  AP02               Probing        N/A   No    802.11a   1
00:09:5b:92:40:e8  AP02               Probing        N/A   No    802.11a   1
00:09:5b:94:2b:80  AP02               Probing        N/A   No    802.11b   1
00:09:5b:a2:74:4e  AP02               Probing        N/A   No    802.11a   1
00:09:5b:c1:bb:bb  AP02               Probing        N/A   No    802.11b   1
00:09:5b:c3:9e:92  AP02               Probing        N/A   No    802.11b   1
00:0b:fc:fc:15:80  AP02               Probing        N/A   No    802.11b   1
00:0c:41:fc:88:53  AP02               Probing        N/A   No    802.11b   1
00:0d:88:9c:ad:47  AP02               Probing        N/A   No    802.11b   1
00:0d:88:a2:0b:e8  AP02               Probing        N/A   No    802.11a   1
00:0f:b5:10:65:17  AP02               Probing        N/A   No    802.11a   1
00:12:00:ef:3d:40  AP02               Probing        N/A   No    802.11b   1
00:12:d9:61:50:20  AP02               Probing        N/A   No    802.11a   1
00:12:d9:61:50:b0  AP02               Probing        N/A   No    802.11a   1
```

Related Commands **show client ap**, **show client detail**, **show client username**, **show exclusionlist**

show client username

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

show client username *username*

Syntax Description

show	Display configurations.
client	Display client data.
username	Cisco Radio.
username	Client's username.

Defaults

None.

Examples

```
> show client username IT_007

MAC Address        AP ID   Status         WLAN Id    Authenticated
-----------------  ------  -------------  ---------  -------------
00:0c:41:0a:33:13  1       Associated     1          No
```

Related Commands

show client ap, **show client detail**, **show client summary**

show country

The Cisco Wireless LAN controller must be configured to comply with the target country's permitted 802.11a and/or 802.11b frequency bands. To display a list of supported countries and their permitted frequency bands, use the **show country** command. This command also shows you the current country setting for the Cisco Wireless LAN controller.

Note Refer to the related product guide for the most up-to-date country codes and regulatory domains.

show country

Syntax Description

show	Display configuration options.
country	Supported Countries.

Defaults

None.

Examples

```
> show country
```

Related Commands

show sysinfo

show database

To display the local database configuration, use the **show database** command.

show database summary

Syntax Description

show database	Command action.
summary	Database summary.

Defaults

None.

Examples

```
> show database summary

Current Max database entries..... 512
Max database entries on next reboot..... 512
```

Related Commands

show sysinfo

show cpu

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

show cpu

Syntax Description

show cpu	Command action.

Defaults

None.

Examples

```
> show cpu

Current CPU load: 2.50%
```

Related Commands

show sysinfo

show custom-web

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

show custom-web

Syntax Description

show custom-web	Command action.

Defaults

None.

Examples

```
> show custom-web

Cisco Logo..................................... Enabled
CustomLogo..................................... Disabled
Custom Title................................... Disabled
Custom Message................................. Disabled
Custom Redirect URL............................ Disabled
External Web Authentication Mode............... Disabled
External Web Authentication URL................ Disabled
External Web Server list
    Index      IP Address
    -----    ---------------
        1            0.0.0.0
        2            0.0.0.0
        3            0.0.0.0
        4            0.0.0.0
        5            0.0.0.0
        6            0.0.0.0
        7            0.0.0.0
        8            0.0.0.0
        9            0.0.0.0
       10            0.0.0.0
       11            0.0.0.0
       12            0.0.0.0
       13            0.0.0.0
       14            0.0.0.0
       15            0.0.0.0
       16            0.0.0.0
       17            0.0.0.0
       18            0.0.0.0
       19            0.0.0.0
       20            0.0.0.0
```

Related Commands

config custom-web

show debug

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

show debug

Syntax Description

show	Display configurations.
debug	MAC address debugging.

Defaults

disabled

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	Display internal DHCP server configuration information.
[leases | summary | *scope***]**	• Enter **leases** to display allocated DHCP leases. • Enter **summary** to display DHCP summary information. • 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 eventlog

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

show eventlog

Syntax Description

show	Display 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 ike

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

show ike {brief | *IP_or_MAC_address***}**

Syntax Description

show	Command action.
ike	Display active IKE SAs.
brief	List of all active IKE SAs.
IP_or_MAC_address	IP or MAC address of active IKE SA.

Defaults

None.

Examples

```
> show ike
```

Related Commands

None

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	Display active IPSec SAs
{brief | *IP_or_MAC_address***}**	Enter **brief** to display active IPSec SAs. Enter the IP address of MAC address of an IPSec SA.

Defaults

None.

Examples

```
> show ipsec brief
```

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	Display a summary of the local interfaces.
detailed	Display detailed interface information.
interface_name	Identifies interface name for detailed display

Defaults

None.

Examples

```
> show interface summary

Interface Name                   Vlan Id   IP Address      Type     Ap Mgr
-------------------------------  --------  --------------  -------  ------

ap-manager                       149       1.100.49.31     Static   Yes
management                       149       1.100.49.30     Static   No
service-port                     N/A       172.19.32.60    Static   No
virtual                          N/A       1.1.1.1         Static   No

> 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
```

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	Display 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
```

Related Commands

show sysinfo

show l2tp

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

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

Syntax Description

show	Display configurations.
summary	Displays all L2TP sessions.
ip_address	Displays an L2TP session.

Defaults

None.

Examples

```
> show l2tp summary

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

Related Commands

None

show known ap

To display known Cisco 1000 Series lightweight access point information, use the **show known ap** command.

show known ap {summary | detailed}

Syntax Description

show	Display configurations.
known ap	Known Cisco 1000 Series lightweight access point information.
summary	Displays a list of all Known APs.
detailed	Provides detailed information for a Known access point.

Defaults

None

Examples

```
> show known ap summary

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

Related Commands

config ap

show location

To display information about defined locations, use the **show location** command.

show location summary

Syntax Description

show location	Display command for locations.
summary	Display all location information defined in the system.

Defaults

None

Examples

```
> show location summary

Status..................................................... disabled
```

Related Commands

config location

show load-balancing

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

show load-balancing

Syntax Description

show	Display configurations.
load-balancing	Display the load-balancing status.

Defaults

None.

Examples

```
> show load-balancing

Aggressive Load Balancing..................... Enabled
Aggressive Load Balancing Window.............. 0 clients
```

Related Commands

config load-balancing

show loginsession

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

show loginsession

Syntax Description

show	Display configurations.
loginsession	Current session details.

Defaults

None.

Examples

```
> show loginsession

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

Related Commands

config loginsession close

show macfilter

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

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

Syntax Description

show	Display configurations.
macfilter	Filter details.
detail *MAC*	Detailed display of a MAC filter entry.
summary	Display a summary of all MAC filter entries.

Defaults

None.

Examples

```
> show macfilter detail 00:0b:85:0e:05:80

MAC Address..................................... 00:0b:85:0e:05:80
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
-----------------------   --------------   --------------------------------
00:0b:85:0e:05:80         Any              RAP
00:0b:85:0e:13:d0         Any              PAP2 (2nd hop)
00:0b:85:0e:14:00         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	Display 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 mesh

To display the mesh configuration for the Cisco Wireless LAN controller, use the **show mesh** command.

show mesh {neigh | path | stats | linkrate | summary}

Syntax Description

show	Display configurations.
mesh	Mesh configuration.
neigh	Show Cisco 1000 Series lightweight access point neighborhood list.
path	Show Cisco 1000 Series lightweight access point path.
stats	Show Cisco 1000 Series lightweight access point statistics
linkrate	Show link rate statistics
summary	Show summary neighbor information for an access point.

Defaults

None.

Examples

```
> show mesh summary
```

Related Commands

None.

SHOW MOBILITY COMMANDS

Use the show mobility commands to display mobility settings.

show mobility statistics

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

show mobility statistics

Syntax Description

show	Display 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
   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 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	Display configurations.
mobility	Mobility group.
anchor	Display the mobility Wireless LAN anchor list.

Defaults

None.

Examples

```
> show mobility anchor
```

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	Display configurations.
mobility	Mobility group.
summary	Display a summary of the Mobility manager.

Defaults

None.

Examples

```
> show mobility summary

Mobility Protocol Port..... 16666
Mobility Security Mode..... Disabled
Default Mobility Domain..... mikemesh
Mobility Group members configured..... 1

Switches configured in the Mobility Group
 MAC Address          IP Address         Group Name
 00:0b:85:32:ab:60    1.100.49.30        <local>
```

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 that 15 entries you are prompted to display the messages shown in the example.

show msglog

Syntax Description

show	Display configurations.
msglog	Show 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 Network Access Control (NAC) detailed information about a Cisco Wireless LAN controller, use the **show nac statistics** command.

show nac statistics

Syntax Description

show	Display configurations.
nac	Network access control.
statistics	Detailed statistics.

Defaults

None.

Examples

```
> show nac statistics

Server Index..................................................... 1
Server Address................................................... 1.1.1.1
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	Display configurations.
nac	Network Access Control.
summary	Summary information

Defaults

None.

Examples

```
> show nac summary

NAC ACL Name ..........................................
Index  Server Address                          Port     State
-----  ---------------------------------------  ----     -----
1      1.1.1.1                                  13336    Enabled
```

Related Commands

show nac acl, **show nac statistics.**

show netuser

To display local network user accounts, use the **show netuser** command.

show netuser

Syntax Description

show	Display configurations.
netuser	Network users.

Defaults

None.

Examples

```
> show netuser

User Name                WLAN Id        Description
------------------------ -------------- --------------------------------
krebbis                    1             all krebbis
```

Related Commands

config netuser add, **config netuser delete**, **config netuser password**, **config netuser wlan-id**

show network

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

show network

Syntax Description

show	Display configurations.
network	Network configuration.

Defaults

None.

Examples

```
> show network

RF-Network Name.............................. mikemesh
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Disable
Ethernet Multicast Mode...................... Disable
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
ARP Unicast Mode............................. Disabled
Cisco AP Default Master...................... Disable
Mgmt Via Wireless Interface.................. Disable
Bridge AP Zero Config........................ Enable
Bridge Shared Secret......................... admin
Allow Old Bridging Aps To Authenticate....... Enable
Over The Air Provisioning of AP's............ Enable
Mobile Peer to Peer Blocking................. Disable
Apple Talk................................... Disable
AP Fallback.................................. Enable
Web Auth Redirect Ports...................... 80
Fast SSID Change............................. Disabled
```

Related Commands

config network arptimeout, **config network bcast-ssid**, **config network dsport**, **config network master-base**, **config network mgmt-via-wireless**, **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 port

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

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

Syntax Description

show	Display configurations.
port	Cisco Wireless LAN controller port.
{*port* **| summary}**	Individual port or all ports

Defaults

None.

Examples

```
> show port 3

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

> show port summary

            STP   Admin    Physical   Physical   Link   Link    Mcast
Pr  Type    Stat   Mode      Mode      Status   Status  Trap   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
```

Related Commands

config ap port, **config network dsport**, **config mirror port**, **config port adminmode**, **config port autoneg**, **config port linktrap**, **config port physicalmode**, **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 qos	Command action
queue_length all	Display 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 pmk-cache

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

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

Syntax Description

show	Display configurations.
pmk-cache	PMK cache.
{all | *MAC***}**	Display information about all entries in the PMK cache, or about a single entry in the PMK cache.

Defaults

None.

Examples

```
> show pmk-cache all

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

Related Commands

config pmk-cache delete

show rfid config

To display RFID tag tracking information, use the **show rfid config** command.

show rfid config

Syntax Description

show	Display configurations.
rfid	Network configuration.
config	Configuration options for RFID tag tracking.

Defaults

None.

Examples

```
> show rfid config

RFID Tag data Collection..................... Enabled
RRID Tag Auto-Timeout........................ Enable
RFID Client data Collection.................. Disabled
RFID data timeout............................ 1200 seconds
```

Related Commands

config rfid, **show rfid summary**, **show rfid detail.**

show rfid detail

To display detailed information about one RFID tag, use the **show rfid detail** command.

show rfid detail *MAC*

Syntax Description

show	Display configurations.
rfid	Network configuration.
detail	Detailed information for one rfid tag.
MAC	Show tag details for this MAC address.

Defaults

None.

Examples

```
> show rfid detail 00:40:96:90:d1:6a
```

Related Commands

config rfid, **show rfid config**, **show rfid summary.**

show rfid summary

To display summary information about all known RFID tag tracking tags, use the **show rfid summary** command.

show rfid summary

Syntax Description

show	Display configurations.
rfid	Network configuration.
summary	Summary information for all known RFID tags.

Defaults

None.

Examples

```
> show rfid summary

    RFID   TYPE   Closest AP    RSSI   Time Since Last Heard
---------- ------ ------------- ------ --------------------
```

Related Commands

config rfid, **show rfid config**, **show rfid detail.**

SHOW RADIUS COMMANDS

Use the show radius commands to display Remote Authentication Dial In User Service (RADIUS) settings.

show radius acct statistics

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

show radius acct statistics

Syntax Description

show	Display 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	Display configurations.
radius auth	RADIUS authentication server.
statistics	Display 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, provide 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	Display configurations.
radius rfc3576	RADIUS RFC3576 server
statistics	Display 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	Display 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 ROGUE AP COMMANDS

Use the rogue access point commands to display rouge 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 *MAC*

Syntax Description

show	Display configurations.
rogue ap	Rogue access point.
clients	Summary information.
MAC	Rogue access point MAC address.

Defaults

None.

Examples

```
> show rogue ap clients 00:0b:85:01:39:13
```

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 *MAC*

Syntax Description

show	Display configurations.
rogue ap	Rogue access point.
detailed	Display detailed information.
MAC	Rogue access point MAC address.

Defaults

None.

Examples

```
> show rogue ap detailed 00:12:44:b4:c6:f0

Rogue BSSID..................................... 00:12:44:b4:c6:f0
Is Rogue on Wired Network....................... No (Unknown if WEP is enabled)
State........................................... Alert
First Time Rogue was Reported.................. Thu Aug  4 16:03:08 2005
Last Time Rogue was Reported................... Thu Aug  4 19:06:08 2005
Reported By
    AP 1
        MAC Address............................ 00:0b:85:18:b6:50
        Name................................... AP02
        Radio Type............................. 802.11a
        SSID................................... vwent
        Channel................................ 60
        RSSI................................... -80 dBm
        SNR.................................... 8 dB
        Encryption............................. Disabled
        ShortPreamble.......................... Disabled
        WPA Support............................ Disabled
        Last reported by this AP............... Thu Aug  4 19:06:08 2005
```

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	Display configurations.
rogue ap	Rogue access point.
summary	Display a list of all Rogue access points.

Defaults

None.

Examples

```
> show rogue ap summary

Rogue Location Discovery Protocol.................  Disabled
RLDP Auto-Contain.................................  Disabled

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- --------- -----------------------
00:02:8a:0e:33:af  Alert               1     0         Thu Aug  4 18:57:11 2005
00:02:8a:0e:33:b0  Alert               1     0         Thu Aug  4 19:00:11 2005
00:02:8a:1f:93:f9  Alert               1     0         Thu Aug  4 18:57:11 2005
00:02:8a:1f:94:15  Alert               1     0         Thu Aug  4 18:57:11 2005
```

Related Commands

show rogue ap detailed, **show rogue ap clients**

SHOW ROGUE ADHOC COMMANDS

Use the rogue adhoc commands rouge 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	Display configurations.
rogue adhoc	Ad hoc Rogue.
detailed	Display detailed information.
MAC	Ad hoc Rogue MAC address.

Defaults

None.

Examples

```
> show rogue adhoc detailed 00:40:96:90:d1:6a

Adhoc Rogue MAC Address...................... 00:40:96:90:d1:6a
State........................................ Alert
First Time Adhoc Rogue was Reported.......... Sat Aug  9 15:48:50 2003
Last Time Adhoc Rogue was Reported........... Sat Aug  9 21:16:50 2003
Reported By
    AP 1
        MAC Address.......................... 00:0b:85:01:88:b0
        Name................................. AP1
        Radio Type........................... 802.11b
        SSID................................. Chichen
        Channel.............................. 6
        RSSI................................. -60 dBm
        SNR.................................. 40 dB
```

Related Commands

show rogue adhoc summary

show rogue adhoc summary

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

show rogue adhoc summary

Syntax Description

show	Display configurations.
rogue adhoc	Adhoc rogue access point.
summary	Displays a list of all Adhoc Rogues.

Defaults

None.

Examples

```
> show rogue adhoc summary

Client MAC Address   Adhoc BSSID    State  # APs      Last Heard
------------------   ----- -----    -----    ---       -------
00:02:6d:28:37:ab                   Alert    1     Sat Aug  9 21:12:50 2004
00:09:6b:54:23:90                   Alert    1     Aug  9 21:12:50 2003
00:0b:65:00:80:40                  Alert     1   Sat Aug  9 21:10:50 2003
```

Related Commands

show rogue adhoc detailed

SHOW ROGUE CLIENT COMMANDS

Use the following rogue client commands to display the rouge 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	Display 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 00:0b:85:01:4c:60

Rogue BSSID..................................... 00:0b:85:01:4c:60
State........................................... Alert
First Time Rogue was Reported................... Thu Aug  4 18:51:08 2005
Last Time Rogue was Reported.................... Thu Aug  4 19:00:08 2005
Rogue Client IP address......................... 192.168.1.117
Reported By
    AP 1
        MAC Address............................. 00:0b:85:18:b6:50
        Name.................................... AP02
        Radio Type.............................. 802.11a
        RSSI.................................... -1 dBm
        SNR..................................... -1 dB
        Channel................................. 56
        Last reported by this AP................ Thu Aug  4 19:00:08 2005
```

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	Display configurations.
rogue client	Rogue client.
summary	Display a list of all Rogue clients.

Defaults

None.

Examples

```
> show rogue client summary

MAC Address        State              # APs Last Heard
-----------------  ------------------ ----- ----------------------
00:02:6f:20:0a:06  Alert              1     Thu Aug  4 19:00:08 2005
00:02:6f:20:0a:07  Alert              1     Thu Aug  4 19:00:08 2005
00:02:6f:20:0a:08  Alert              1     Thu Aug  4 19:00:08 2005
00:02:6f:22:0d:03  Alert              1     Thu Aug  4 19:00:08 2005
00:02:6f:22:0d:04  Alert              1     Thu Aug  4 19:00:08 2005
00:02:6f:22:0d:05  Alert              1     Thu Aug  4 19:00:08 2005
00:09:5b:c1:bb:bb  Alert              1     Thu Aug  4 19:09:11 2005
00:09:5b:c3:9e:92  Alert              1     Thu Aug  4 19:03:11 2005
00:0b:85:01:3a:c1  Alert              1     Thu Aug  4 19:03:11 2005
00:0e:35:57:c3:b5  Alert              1     Thu Aug  4 19:09:11 2005
00:0f:b5:11:49:87  Alert              1     Thu Aug  4 18:57:08 2005
00:12:7f:79:74:b7  Alert              1     Thu Aug  4 19:12:08 2005
```

Related Commands

show rogue client detailed

show route summary

To a 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	Display all the configured routes.

Defaults

None.

Examples

```
> show route summary

Number of Routes.............................. 1

Destination Network          Genmask               Gateway
-------------------    -------------------   -------------------
193.122.17.3           255.255.255.0         172.99.3.89
```

Related Commands

config route

show rules

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

show rules

Syntax Description

show rules	Display active internal firewall rules.

Defaults

None.

Examples

```
> show rules

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

Related Commands

None.

show run-config

To a 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...................................  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

Press Enter to continue
```

Related Commands

config route

show serial

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

show serial

Syntax Description

show	Display configurations.
serial	Display 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 a show the console port login timeout and maximum number of simultaneous CLI sessions, use the **show sessions** command.

show sessions

Syntax Description

show	Display configurations.
sessions	Display CLI session configuration information.

Defaults

5 minutes, 5 sessions.

Examples

```
> show sessions

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

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

Related Commands

config sessions maxsessions, **config sessions timeout**

show snmpcommunity

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

show snmpcommunity

Syntax Description

show	Display configurations.
snmpcommunity	Display 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 a show the Cisco Wireless LAN controller SNMP trap receivers and their status, use the **show snmptrap** command.

show snmptrap

Syntax Description

show	Display configurations.
snmptrap	SNMP trap receivers.

Defaults

None.

Examples

```
> show snmptrap

SNMP Trap Receiver Name    IP Address        Status
-------------------------  ----------------- --------
180.16.19.81               172.16.16.81      Enable
```

Related Commands

config snmp version, **config snmp trapreceiver**

show snmpv3user

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

show snmpv3user

Syntax Description

show	Display configurations.
snmpv3user	SNMP version 3 configuration information.

Defaults

None.

Examples

```
> show snmpv3user

SNMP v3 User Name    AccessMode  Authentication Encryption
-------------------- ----------- -------------- ----------
default              Read/Write  HMAC-MD5       CBC-DES
```

Related Commands

config snmp version, **config snmp v3user**

show snmpversion

To a show the SNMP version status, use the **show snmpversion** command.

show snmpversion

Syntax Description

show	Display configurations.
snmpversion	Display 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 a 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	Display configurations.
spanningtree	Spanning tree.
port	Display spanning tree values on a per port basis.
port	Physical port number: • 1 through 4 on Cisco 2000 Series Wireless LAN controller. • 1 or 2 on Cisco 4100 Series Wireless LAN controller. • 1 or 2 on Cisco 4402 Series Wireless LAN controller. • 1 through 4 on Cisco 4404 Series Wireless LAN controller.

Defaults

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

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

show spanningtree switch

Syntax Description

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

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 STATS COMMANDS

Use the show stats commands to display controller statistics.

show stats port

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

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

Syntax Description

show	Display configurations.
stats	Statistics.
port	Port.
detailed	Display detailed port statistics.
summary	Display port summary statistics.
port	Physical port number: • 1 through 4 on Cisco 2000 Series Wireless LAN controllers. • 1 or 2 on Cisco 4100 Series Wireless LAN controllers. • 1 or 2 on Cisco 4402 Series Wireless LAN controllers. • 1 through 4 on Cisco 4404 Series Wireless LAN controllers.

Defaults

None.

Examples

```
> show stats port summary 5

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 5

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

...
```

Related Commands

config port physicalmode

show stats switch

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

show stats switch {detailed | summary}

Syntax Description

show	Display configurations.
stats	Statistics.
switch	Cisco Wireless LAN controller.
detailed	Display detailed switch statistics.
summary	Display 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.......................................... 13973582
Total Pkts...................................... 136441
Unicast Pkts.................................... 117636
Multicast Pkts.................................. 0
Broadcast Pkts.................................. 18805
Pkts Discarded.................................. 0

TRANSMIT
Octets.......................................... 5919784
Total Pkts...................................... 78028
Unicast Pkts.................................... 33448
Multicast Pkts.................................. 41240
Broadcast Pkts.................................. 3340
Pkts Discarded.................................. 2

ADDRESS ENTRIES
Most Ever Used.................................. 26
Currently In Use................................ 26
...
```

Related Commands

config network dsport

show switchconfig

To display parameters that apply to the switch (for example, the network (DS port) 802.3x flow control mode) **use the show switchconfig** command.

show switchconfig

Syntax Description

show	Display configurations.
switchconfig	Display parameters that apply to the switch.

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

show sysinfo

Syntax Description

show	Display configurations.
sysinfo	Cisco Wireless LAN controller information.

Defaults

None.

Examples

```
> 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
```

Related Commands

config country, **config wlan**, **config ap**

show syslog

To a show the Cisco Wireless LAN controller SNMP trap logging status or target IP Address, use the **show syslog** command.

show syslog

Syntax Description

show	Display configurations.
syslog	Display the state of system syslog.

Defaults

None.

Examples

```
> show syslog

Syslog destination.............................. disabled

> show syslog

Syslog destination.............................. 10.10.2.7
```

Related Commands

config syslog

show tech-support

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

show tech-support

Syntax Description

show	Display configurations.
tech-support	Display 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 a show the Cisco Wireless LAN controller time and date, use the **show time** command.

show time

Syntax Description

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

show trapflags

Syntax Description

show	Display configurations.
trapflags	Display 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 WLAN Solution 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 a show the Cisco Wireless LAN controller SNMP trap log, use the **show traplog** command.

show traplog

Syntax Description

show	Display 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 watchlist

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

show watchlist

Syntax Description

show	Command action.
watchlist	Display client watchlist entry.

Defaults

None.

Examples

```
> show watchlist

client watchlist state is disabled
```

Related Commands

config watchlist delete, **config watchlist enable, config watchlist disable**, **config watchlist add**

show wlan

To show WPS configuration information, use the **show wlan summary** command.

show wlan {mobility | summary | *wlan_id* **| foreignAp}**

Syntax Description

show	Display configurations.
wlan	Wireless LAN.
mobility	Display mobility management configuration.
summary	Displays a summary of all Wireless LANs.
wlan_id	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
Network Name (SSID).......................... Controller
Status....................................... Enabled
MAC Filtering................................ Disabled
AAA Policy Override.......................... Disabled
Network Access Control....................... Disabled
Number of Active Clients..................... 1
Exclusionlist................................ Disabled
Session Timeout.............................. Infinity
Interface.................................... management
DHCP Server.................................. 10.1.2.119
Quality of Service........................... Bronze (low)
WMM.......................................... Allowed
802.11e...................................... Disabled
Wired Protocol............................... None
IPv6......................................... Disabled
Radio Policy................................. All
Security
--More-- or (q)uit

> show wlan summary

Number of WLANs.............................. 1

WLAN ID  WLAN Name             Status
------- ---------------------- ---------
1       mjoyce4404             Enabled
```

Related Commands

config wlan blacklist, **config wlan create**, **config wlan delete**, **config wlan dhcp_server**, **config wlan disable**, **config wlan enable**, **config wlan mac-filtering**, **config wlan qos**, **config wlan radio**, **config wlan security 802.1X**, **config wlan security 802.1X encryption**, **config wlan security cranite**, **config wlan security ipsec**, **config wlan security ipsec authentication**, **config wlan security ipsec encryption**, **config wlan security ipsec ike authentication**, **config wlan security ipsec ike DH-Group**,

config wlan security ipsec ike lifetime, **config wlan security ipsec ike phase1**, **config wlan security passthru**, **config wlan security static-wep-key**, **config wlan security static-wep-key encryption**, **config wlan security web**, **config wlan security web passthru**, **config wlan security wpa**, **config wlan security wpa encryption**, **config wlan timeout**

Setting Configurations

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

CONFIG 802.11A COMMANDS

Use the config 802.11a commands to configure 802.11a settings.

config 802.11a antenna extAntGain

To configure the 802.11a external antenna gain, use the **config 802.11a antenna extAntGain** command.

Use the **config 802.11a disable** command to disable the 802.11a Cisco Radio before using the **config 802.11a antenna** command. After configuring the external antenna gain, use the **config 802.11a enable** command to enable the 802.11a Cisco Radio.

config 802.11a antenna extAntGain *antenna_gain Cisco_AP*

Syntax Description

config	Configure parameters.
802.11a antenna	Antennas for 802.11a Cisco Radio.
antenna_gain	Enter antenna gain in 0.5 dBm units.
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

None.

Examples

To set AP1 to use the 802.11a internal antennas:

```
> config 802.11a antenna extAntGain 1 AP02
```

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 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 1000 Series lightweight access point right port.
sideB	Between the internal antennas and an external antenna connected to the Cisco 1000 Series lightweight access point left port.
Cisco_AP	Cisco 1000 Series 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 1000 Series 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 1000 Series 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.
Cisco_AP	Cisco 1000 Series IEEE 802.11a/b/g 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 selection	Antenna selection (internal or external) for 802.11a.
internal	Select internal antennas.
external	Select external antenna.
Cisco_AP	Cisco 1000 Series 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 1000 Series 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 Cisco 1000 Series 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.
time_units	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 for automatic or manual channel selection, use the **config 802.11a channel** command.

When configuring 802.11a channels for a single Cisco 1000 Series 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 Cisco Radio. Then enable the 802.11a network using the config 802.11a enable command.

config 802.11a channel {global {auto | once | off} | *Cisco_AP* **{global |** *channel***}}**

Syntax Description

config	Configure parameters.
802.11a channel	Cisco Radio channel number.
global {auto | once | off}	Global channel control: • Enter **auto** to enable auto-RF. • Enter **once** to enable one-time auto-RF. • Enter **off** to disable auto-RF and set all channels to default.
Cisco_AP **{global |** *channel***}**	Name of Cisco 1000 Series lightweight access point or global setting for all Cisco 1000 Series lightweight access points. • Enter **global** to enable auto-RF. • Enter a channel number to set the default channel.

Defaults

None.

Examples

To have RRM automatically configure all 802.11a channels based on availability and interference:

```
> config 802.11a channel global auto
```

To have RRM automatically reconfigure all 802.11a channels one time based on availability and interference:

```
> config 802.11a channel global once
```

To turn 802.11a RRM automatic configuration off:

```
> config 802.11a channel global off
```

To configure all 802.11a channels in AP01:

```
> config 802.11a channel AP01 global
```

To configure 802.11a channel 36 in AP01 as the default channel:

```
> config 802.11a channel AP01 36
```

Related Commands

show 802.11a, **config 802.11a disable**, **config 802.11a enable**, **config 802.11b channel**

config 802.11a 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 commands.

config 802.11a disable {network | *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.
Cisco_AP	Disables transmission for an individual Cisco 1000 Series lightweight access point Cisco Radio.

Defaults

Transmission is enabled for the entire network by default.

Examples

To disable the whole 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 dtim

In 802.11 networks, the Cisco 1000 Series lightweight access point Wireless LANs broadcast a beacon at regular intervals, which coincides with the DTIM (Delivery Traffic Indication Map). After the DTIM, if the Cisco 1000 Series lightweight access point has any frames buffered for broadcast or multicast, it transmits the buffered frames. This protocol allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Normally, the DTIM value is set to 1 (transmit broadcast and multicast after every beacon) or 2 (transmit after every other beacon). For instance, if the beaconperiod is 100 ms, and the DTIM value is set to 1, the Cisco 1000 Series lightweight access point transmits buffered broadcast and multicast frames 10 times a second; if the beaconperiod is 100 ms, and the DTIM value is set to 2, the Cisco 1000 Series lightweight access point transmits buffered broadcast and multicast frames five times a second; either of these settings may be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (transmit broadcast and multicast after every 255th beacon), if all 802.11a clients have power save enabled. Because the clients only have to listen when the DTIM time is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in longer battery life. For instance, if the beaconperiod is 100 ms, and the DTIM value is set to 100, the Cisco 1000 Series lightweight access point transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power saving clients to sleep longer between periods when they have to wake up and listen for broadcasts and multicasts, resulting in longer battery life.

Many applications cannot tolerate a long time between broadcast and multicast messages, resulting in poor protocol and application performance. A low DTIM value is indicated for 802.11a networks that support such clients.

To change the DTIM value for the whole 802.11a network, use the **config 802.11a dtim** command.

config 802.11a dtim *period*

Syntax Description

config	Configure parameters.
802.11a	802.11a network parameters.
dtim	Delivery Traffic Indication Map.
period	DTIM value in number of beaconperiods.

Defaults

1 (every beaconperiod)

Examples

To configure the 802.11a network to transmit multicast and broadcast messages every other DTIM, or beaconperiod:

```
> config 802.11a dtim 2
```

Related Commands

show 802.11a, **config 802.11a beaconperiod**, **config 802.11b dtim**, **config 802.11a disable**, **config 802.11a enable**

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 dtim**, **config 802.11a disable**, **config 802.11a enable**

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.
threshold	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 enable

Enable 802.11a transmissions for the whole network or for an individual Cisco 1000 Series 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 | *Cisco_AP***}**

Syntax Description

config	Configure parameters.
802.11a	802.11a network parameters.
enable	Disables/enables 802.11a.
network	For the whole network.
Cisco_AP	Override the network setting for an individual Cisco 1000 Series lightweight access point Cisco 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 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 1000 Series IEEE 802.11a/b/g 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 Tx (transmit) power level, use the **config 802.11a txPower** command.

config 802.11a txPower {global {auto | once | *power_level***} |** *Cisco_AP* **{global |** *power_level***}}**

Syntax Description

config	Configure parameters.
802.11a	802.11a network parameters.
txPower	Transmit power parameter.
global	All Cisco 1000 Series lightweight access points.
auto	Periodic RRM automatic configuration.
once	Enable one-time auto-RF.
Cisco_AP	Cisco 1000 Series IEEE 802.11a/b/g lightweight access point name.
power_level	Transmit power level number. The supported number of levels depends on the access point used. For example, the 1240 access point supports 8 levels and the 1200 access point supports 6 levels. **Note** Refer to the related product guide for the maximum regulatory transmit power level limits published for each country code. The power levels and available channels are defined by the country code setting, and are regulated on a country by country basis. Also, the actual maximum transmit power levels may be less than the published regulatory limits.

Defaults

Global, Auto.

Examples

To have RRM automatically set the transmit power for all 802.11a Cisco Radios at periodic intervals:

```
> config 802.11a txPower global auto
```

To set transmit power for all 802.11a Cisco Radios to power level 5:

```
> config 802.11a txPower global 5
```

To set transmit power for 802.11a AP1 to global:

```
> config 802.11a txPower AP1 global
```

To set transmit power for 802.11a AP1 to power level 2:

```
> config 802.11a txPower AP1 2
```

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 802.11b settings.

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 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 802.11a Cisco Radio.

config 802.11b antenna extAntGain *antenna_gain Cisco_AP*

Syntax Description

config	Configure parameters.
802.11a antenna	Antennas for 802.11a/g Cisco Radio.
antenna_gain	Enter antenna gain in 0.5 dBm units.
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

None.

Examples

To set AP1 to use the 802.11b internal antennas:

```
> config 802.11b antenna extAntGain 1 AP02
```

Related Commands

config 802.11b disable, **config 802.11b enable**, **config 802.11b diversity**, **config 802.11b selection**.

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 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 1000 Series lightweight access point Left port.
sideB	Between the internal antennas and an external antenna connected to the Cisco 1000 Series lightweight access point Right port.
Cisco_AP	Cisco 1000 Series 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 1000 Series 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 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 selection	Antenna selection (internal or external) for 802.11b.
internal	Select internal antennas.
external	Select external antenna.
Cisco_AP	Cisco 1000 Series 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 1000 Series 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 1000 Series 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 *milliseconds*

Syntax Description

config	Configure parameters.
802.11b	802.11b/g network parameters.
beaconperiod	Send a beacon every 20 to 1000 milliseconds.
milliseconds	Beacon interval in milliseconds.

Defaults

100 milliseconds.

Examples

To configure an 802.11b/g network for a beacon period of 180 milliseconds:

```
> 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 the 802.11b/g network for automatic or manual channel selection, use the **config 802.11b channel** command.

When configuring 802.11b/g channels for a single Cisco 1000 Series lightweight access point, use the config 802.11b disable command to disable the 802.11b/g network. Then use the config 802.11b channel command to set automatic channel selection by RRM or manually set the channel for the 802.11b/g Cisco Radio. Then enable the 802.11b/g network using the config 802.11b enable command.

config 802.11b channel {global {auto | once | off}} | {*Cisco_AP* **{global |** *channel***}}**

Syntax Description

config	Configure parameters.
802.11b channel	802.11b/g Cisco Radio channel number.
global	Global channel control.
Cisco_AP	Name of Cisco 1000 Series lightweight access point or global setting for all Cisco 1000 Series lightweight access points.

Defaults

None.

Examples

To have RRM automatically configure all 802.11b/g channels based on availability and interference:

```
> config 802.11b channel global auto
```

To have RRM automatically reconfigure all 802.11b/g channels one time based on availability and interference:

```
> config 802.11b channel global once
```

To turn 802.11b/g RRM automatic configuration off:

```
> config 802.11b channel global off
```

To have AP1 use the global (whole network) settings.

```
> config 802.11b channel AP1 global
```

To have AP1 start and continue using channel 11.

```
> config 802.11b channel AP1 channel 11
```

Only channels 1, 6 and 11 are nonoverlapping.

Related Commands

show 802.11b, **config 802.11b disable**, **config 802.11b enable**, **config 802.11a channel**

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.
Cisco_AP	Override the network setting for an individual Cisco 1000 Series lightweight access point Cisco 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 802.11b**, **config 802.11a disable**, **config 802.11a enable**, **config 802.11b enable**, **config 802.11b beaconperiod**

config 802.11b dtim

In 802.11 networks, the Cisco 1000 Series lightweight access point Wireless LANs broadcast a beacon at regular intervals, which coincide with the DTIM. After the DTIM, if the Cisco 1000 Series lightweight access point has any frames buffered for broadcast or multicast, it transmits the buffered frames. This protocol allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Normally, the DTIM value is set to 1 (transmit broadcast and multicast after every beacon) or 2 (transmit after every other beacon). For instance, if the 802.11b/g beaconperiod is 100 ms, and the DTIM value is set to 1, the Cisco 1000 Series lightweight access point transmits buffered broadcast and multicast frames 10 times a second; if the beaconperiod is 100 ms, and the DTIM value is set to 2, the Cisco 1000 Series lightweight access point transmits buffered broadcast and multicast frames five times a second; either of these settings may be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (transmit broadcast and multicast after every 255th beacon), if all 802.11a clients have power save enabled. Because the clients only have to listen when the DTIM time is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in longer battery life. For instance, if the 802.11b/g beaconperiod is 100 ms, and the DTIM value is set to 100, the Cisco 1000 Series lightweight access point transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power saving clients to sleep longer between periods when they have to wake up and listen for broadcasts and multicasts, resulting in longer battery life.

Note that many applications cannot tolerate a long time between broadcast and multicast messages, resulting in poor protocol and application performance. A low DTIM value is indicated for 802.11b/g networks that support such clients.

To change the DTIM value for the whole 802.11b/g network, use the **config 802.11b dtim** command.

Before you change the 802.11b/g DTIM value using the config 802.11b dtim 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 DTIM value, remember to enable the 802.11b/g network using the config 802.11b enable command.

config 802.11b dtim *period*

Syntax Description

config	Configure parameters.
802.11b	802.11b/g network parameters.
dtim	Delivery Traffic Indication Map.
period	DTIM period in number of beaconperiods.

Defaults

1 (every beaconperiod)

Examples

To configure the 802.11b/g network to transmit multicast and broadcast messages every DTIM, or beaconperiod:

```
> config 802.11b dtim 1
```

Related Commands **show 802.11b**, **config 802.11b beaconperiod**, **config 802.11a dtim**, **config 802.11b disable**, **config 802.11b enable**

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 dtim**, **config 802.11b disable**, **config 802.11b enable**

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.
threshold	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 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 | *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.
Cisco_AP	To override the network setting for individual Cisco 1000 Series lightweight access point Cisco 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 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 {short | long}

Syntax Description

config	Configure parameters.
802.11b	802.11b network parameters.
preamble	As defined in subclause 18.2.2.2.
{short | long}	Short or long 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 1000 Series IEEE 802.11a/b/g 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.
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	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/g Tx (Transmit) Power Level, use the **config 802.11b txPower** command.

config 802.11b txPower {global {auto | *power_level***}** | *Cisco_AP* **{global** | *power_level***}}**

Syntax Description

config	Configure parameters.
802.11b	802.11b/g network parameters.
txPower	Transmit power parameter.
global	All Cisco 1000 Series lightweight access points.
auto	Periodic RRM automatic configuration.
Cisco_AP	Cisco 1000 Series IEEE 802.11a/b/g lightweight access point name.
power_level	Transmit power level number. The supported number of levels depends on the access point used. For example, the 1240 access point supports 8 levels and the 1200 access point supports 6 levels.

Note Refer to the related product guide for the maximum regulatory transmit power level limits published for each country code. The power levels and available channels are defined by the country code setting, and are regulated on a country by country basis. Also, the actual maximum transmit power levels may be less than the published regulatory limits.

Defaults

Global, Auto.

Examples

To have RRM automatically set the transmit power for all 802.11b/g Cisco Radios at periodic intervals:

```
> config 802.11a txPower global auto
```

To have RRM automatically reset the transmit power for all 802.11b/g Cisco Radios one time:

```
> config 802.11b txPower global once
```

To set transmit power for all 802.11b/g Cisco Radios to power level 5:

```
> config 802.11b txPower global 5
```

To set transmit power for 802.11b/g AP1 to global:

```
> 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 acl

To configure Access Control Lists, use the **config acl** command.

config acl {apply | create | delete | rule *rule_option***}** *rule_name*

Note For a Cisco 2000 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 4100 Series Wireless LAN controllers and Cisco 4400 Series Wireless LAN controllers.

Syntax Description

config acl	Command action.
apply *name*	Applies the ACL (name with up to 32 alphanumeric characters) to the data path.
create	Create a new ACL.
delete	Delete an ACL.
rule *rule_option*	Enter one of the following rules: • **action** to configure a rule's action. • **add** to add a new rule. • **change** to change a rule's index. • **delete** to delete a rule. • **destination** to configure a rule's destination IP address, netmask and port range. • **direction** to configure a rule's direction. • **dscp** to configure a rule's DSCP. • **protocol** to configure a rule's IP Protocol. • **source** to configure a rule's source IP address, netmask and port range. • **swap** to swap two rules' indices.
rule_name	ACL name up to 32 alphanumeric characters.

Defaults

None.

Examples

```
> config acl create acl01
```

Related Commands

show acl

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 1000 Series 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 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 1000 Series 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 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 ADVANCED 802.11A COMMANDS

Use the advanced 802.11a commands to configure advanced 802.11a settings.

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 1000 Series 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 1000 Series 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 1000 Series 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 Cisco 1000 Series lightweight access point 802.11a load avoidance in the channel assignment. Disable Cisco 1000 Series 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 1000 Series 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 1000 Series 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 1000 Series 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 1000 Series 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 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.
seconds	Coverage measurement interval between 60 and 3600 seconds.

Defaults

180 seconds.

Examples

To set the coverage measurement interval to 60 seconds:

```
> config advanced 802.11a 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.
seconds	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.
seconds	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.
seconds	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 receiver

To set the advanced receiver configuration, use the **config advanced 802.11a receiver** command.

config advanced 802.11a receiver {default | rxstart}

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
receiver	Receiver configuration.
{default | rxstart}	Default advanced receiver configuration. Advanced receiver start configuration.

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 txpower-update

To initiate updates of the 802.11a transmit power for every Cisco 1000 Series 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

config advanced 802.11a profile clients

To set the Cisco 1000 Series IEEE 802.11a/b/g 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 1000 Series lightweight access point Client profile
{global | *Cisco_AP***}**	• Enter **global** to configure all 802.11a Cisco 1000 Series lightweight access points. • Enter a Cisco 1000 Series lightweight access point name.
clients	802.11a Cisco 1000 Series lightweight access point clients threshold between 1 and 75 clients.

Defaults

12 clients.

Examples

To set all Cisco 1000 Series 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 coverage

To set the Cisco 1000 Series lightweight access point coverage threshold between 3 and 50 dB, use the **config advanced 802.11a profile coverage** command.

config advanced 802.11a profile coverage {global | *Cisco_AP***}** *dBm*

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
profile coverage	Cisco 1000 Series lightweight access point profile coverage
{global | *Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile.
dBm	3 to 50 dB.

Defaults

12 dB.

Examples

To set all Cisco 1000 Series lightweight access point coverage thresholds to 30 dB:

```
> config advanced 802.11a profile coverage global 30
```

To set AP1 coverage thresholds to 50 dB:

```
> config advanced 802.11a profile coverage AP1 50
```

Related Commands

show advanced 802.11a profile, **config advanced 802.11b profile coverage**

config advanced 802.11a profile customize

To turn customizing on or off for an 802.11a Cisco 1000 Series 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 1000 Series lightweight access point.
on/off	Enter **on** to customize performance profiles for this Cisco 1000 Series lightweight access point. Enter **off** to use global default performance profiles for this Cisco 1000 Series lightweight access point.

Defaults

Off.

Examples

To turn performance profile customization on for 802.11a Cisco 1000 Series 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 exception

To set the Cisco 1000 Series lightweight access point coverage exception level between 0 and 100 percent, use the **config advanced 802.11a profile exception** command.

config advanced 802.11a profile exception {global | *Cisco_AP***}** *percent*

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
profile exception	Cisco 1000 Series lightweight access point profile exception
{global | *Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile.
percent	802.11a Cisco 1000 Series lightweight access point coverage exception level between 0 and 100 percent.

Defaults

25 percent.

Examples

To set all Cisco 1000 Series lightweight access point coverage exception levels to 0 percent:

```
> config advanced 802.11a profile exception global 0
```

To set the AP1 coverage exception level to 100 percent:

```
> config advanced 802.11a profile exception AP1 100
```

Related Commands

show advanced 802.11a profile, **config advanced 802.11b profile exception**

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 | *Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile.
percent	802.11a foreign 802.11a interference threshold between 0 and 100 percent.

Defaults

10.

Examples

To set the Other 802.11a transmitter interference threshold for all Cisco 1000 Series 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 level

To set the Cisco 1000 Series lightweight access point client minimum exception level between 1 and 75 clients, use the **config advanced 802.11a profile level** command.

config advanced 802.11a profile level {global | *Cisco_AP***}** *clients*

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
profile level	Cisco 1000 Series lightweight access point profile level
{global	*Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile.
clients	802.11a Cisco 1000 Series lightweight access point client minimum exception level between 1 and 75 clients.

Defaults

3 clients.

Examples

To set all Cisco 1000 Series lightweight access point client minimum exception levels to 10 clients:

```
> config advanced 802.11a profile level global 10
```

To set the AP1 client minimum exception level to 25 clients:

```
> config advanced 802.11a profile level AP1 25
```

Related Commands

show advanced 802.11a profile, **config advanced 802.11b profile level**

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***}** *value*

Syntax Description

config	Configure parameters.
advanced 802.11a	Advanced 802.11a parameters.
profile noise	Profile noise limits
{global | *Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile.
value	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 1000 Series 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 1000 Series 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.
{global | *Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile.
value	802.11a Cisco 1000 Series lightweight access point throughput threshold between 1000 and 10000000 bytes per second.

Defaults

1,000,000 bytes per second.

Examples

To set all Cisco 1000 Series 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 1000 Series lightweight access point profile utilization
{global | *Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile.
percent	802.11a RF utilization threshold between 0 and 100 percent.

Defaults

80 percent.

Examples

To set the RF utilization threshold for all Cisco 1000 Series 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 802.11B 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.
limit	Call admission limit (from 0 to 255). The default value is 105.
quantum	G711 quantum value. The default value is 15.

Defaults

None.

Examples

```
> config advanced 802.11b 7920VSIEConfig call-admission-limit 4
```

Related Commands

None.

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 1000 Series 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 1000 Series 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 1000 Series 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 1000 Series 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 1000 Series 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 1000 Series 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 1000 Series 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 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

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.
seconds	Coverage measurement interval between 60 and 3600 seconds.

Defaults

180 seconds.

Examples

To set the coverage measurement interval to 60 seconds:

```
> config advanced 802.11b 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.
seconds	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.
seconds	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.
seconds	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 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 txpower-update

To initiate updates of the 802.11b transmit power for every Cisco 1000 Series 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 802.11b profile clients

To set the number of 802.11b/g Cisco 1000 Series 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 | *Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile.
clients	802.11b Cisco 1000 Series lightweight access point clients threshold between 1 and 75 clients.

Defaults

12 clients

Examples

To set the Cisco 1000 Series lightweight access point clients threshold for all Cisco Radios to 25:

```
> config advanced 802.11b profile clients global 25
```

To set the Cisco 1000 Series 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 coverage

To set the 802.11b/g Cisco 1000 Series lightweight access point coverage threshold between 3 and 50 dB, use the **config advanced 802.11b profile coverage** command.

config advanced 802.11b profile coverage {global | *Cisco_AP dBm***}**

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
profile coverage	Cisco 1000 Series lightweight access point profile coverage
{global | *Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile
dBm	802.11b Cisco 1000 Series lightweight access point coverage threshold between 3 and 50 dB.

Defaults

12 dB

Examples

To set the Cisco 1000 Series lightweight access point coverage threshold for all Cisco 1000 Series lightweight access points to 30 dB:

```
> config advanced 802.11b profile coverage global 30
```

To set the Cisco 1000 Series lightweight access point coverage threshold for AP1 to 50 dB:

```
> config advanced 802.11b profile coverage AP1 50
```

Related Commands

config advanced 802.11a profile coverage

config advanced 802.11b profile customize

To turn customization on or off for an 802.11b/g Cisco 1000 Series 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 1000 Series lightweight access point.
Cisco_AP	Cisco 1000 Series lightweight access point name.
{on | off}	• Enter **on** to customize performance profiles for the specified Cisco 1000 Series lightweight access point. • Enter **off** to use global default performance profiles for the specified Cisco 1000 Series 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 exception

To set the 802.11b/g Cisco 1000 Series lightweight access point coverage exception level between 0 and 100 percent, use the **config advanced 802.11b profile exception** command.

config advanced 802.11b profile exception {global | *Cisco_AP***}** *percent*

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
profile exception	Cisco 1000 Series lightweight access point profile exception
{global | *Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile
percent	802.11b Cisco 1000 Series lightweight access point coverage exception level between 0 and 100 percent.

Defaults

25%

Examples

To set the Cisco 1000 Series lightweight access point coverage exception level for all Cisco 1000 Series lightweight access points to 0 percent:

```
> config advanced 802.11b profile exception global 0
```

To set the Cisco 1000 Series lightweight access point coverage exception level for AP1 to 100 percent:

```
> config advanced 802.11b profile exception AP1 100
```

Related Commands

config advanced 802.11a profile exception

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	*Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile.
percent	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 level

To set the 802.11b/g Cisco 1000 Series lightweight access point client minimum exception level between 1 and 75 clients, use the **config advanced 802.11b profile level** command.

config advanced 802.11b profile level {global | *Cisco_AP***}** *clients*

Syntax Description

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
profile minimum	Cisco 1000 Series lightweight access point profile level
{global | *Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile
clients	802.11b Cisco 1000 Series lightweight access point client minimum exception level between 1 and 75 clients.

Defaults

3 clients

Examples

To set the Cisco 1000 Series lightweight access point client minimum exception level for all Cisco Radios to 75 clients:

```
> config advanced 802.11b profile level global 75
```

To set the Cisco 1000 Series lightweight access point client minimum exception level for AP1 to 25 clients:

```
> config advanced 802.11b profile level AP1 25
```

Related Commands

config advanced 802.11a profile level

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 1000 Series lightweight access point profile noise
{global | *Cisco_AP***}**	Global or Cisco 1000 Series 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 1000 Series 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.
{global	*Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile.
rate	1,000 to 10,000,000 bps.

Defaults

1,000,000 bps

Examples

To set the Cisco 1000 Series lightweight access point throughput threshold for all Cisco Radios to 1000 bytes per second:

```
> config advanced 802.11b profile throughput global 1000
```

To set the Cisco 1000 Series lightweight access point throughput threshold for AP1 to 10000000 bytes per second:

```
> config advanced 802.11b profile throughput AP1 10000000
```

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 1000 Series lightweight access point profile utilization
{global | *Cisco_AP***}**	Global or Cisco 1000 Series lightweight access point specific profile
percent	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 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.
num_of_retries	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 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**

CONFIG ADVANCED TIMERS COMMANDS

User the advanced timers commands to configure advanced 802.11a settings.

config advanced timers ap-discovery-timeout

The Cisco 1000 Series lightweight access point discovery time-out is how often a Cisco Wireless LAN controller attempts to discover unconnected Cisco 1000 Series lightweight access points. To configure the Cisco 1000 Series 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 1000 Series lightweight access point discovery timeout.
seconds	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-heartbeat-timeout

The Cisco 1000 Series lightweight access point heartbeat timeout controls how often the Cisco 1000 Series lightweight access point sends a heartbeat keep-alive signal to the Cisco Wireless LAN controller. To configure the Cisco 1000 Series 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 1000 Series lightweight access point heartbeat timeout.
seconds	Timeout value between 1 and 30 seconds.

Defaults

30 seconds.

Examples

```
> config advanced timers ap-heartbeat-timeout 20
```

Related Commands

show advanced timers

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.
seconds	Timeout value in seconds between 5 and 600.

Defaults

10 seconds.

Examples

```
> config advanced timers auth-timeout 20
```

Related Commands

show advanced timers

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.
seconds	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.

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

Syntax Description

show	Display configurations.
advanced	Advanced parameters.
timers eap-identity-request-delay	Advanced system timers.
seconds	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**

CONFIG AP COMMANDS

Use the following config ap commands:

config ap add

To add a Foreign Access Point, use the **config ap add** command.

config ap *MAC port* **{enable | disable}** *IP_address*

Syntax Description

config	Display configurations.
ap	Advanced parameters.
add	Add a Foreign Access Point.
MAC	Foreign Access Point MAC address.
port	Port number for accessing the Foreign Access Point.
{enable | disable}	Enable or disable 802.1X authentication for a Foreign Access Point.
IP_address	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 bhrate

To configure the Cisco Bridge Backhaul Tx Rate, use the **config ap bhrate** command.

config ap bhrate *rate Cisco_AP*

Syntax Description

config	Display configurations.
ap	Advanced parameters.
bhrate	Configure Cisco Bridge Backhaul Tx Rate.
rate	Cisco Bridge Backhaul Tx Rate in Kbps. The legal values are: 6000, 12000, 18000, 24000, 36000, 48000, and 54000.
Cisco_AP	Name of a Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config ap bhrate 54000 AP01
```

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}

Syntax Description

config	Display 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.

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 bridgegroupname

To set or delete bridgegroupname on a Cisco 1000 Series 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	Display configurations.
ap	Advanced parameters.
bridgegroupname	Set or delete bridgegroupname on a Cisco 1000 Series lightweight access point
{set *groupname* **| delete}**	• Enter **set** *groupname* to set a Cisco 1000 Series lightweight access point's bridgegroupname. • Enter **delete** to delete a Cisco 1000 Series lightweight access point's bridgegroupname.
Cisco_AP	Name of a Cisco 1000 Series 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 1000 Series lightweight access point, use the **config ap bridging** command.

config ap bridging {enable | disable} *Cisco_AP*

Syntax Description

config	Display configurations.
ap	Advanced parameters.
bridging	enable or disable Ethernet-to-Ethernet bridging on a Cisco 1000 Series lightweight access point.
{enable | disable}	Enable or disable Ethernet-to-Ethernet bridging.
Cisco_AP	Name of a Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

>

Related Commands

config ap

config ap core-dump

To configure a Cisco 1000 Series 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	Display configurations.
ap	Advanced parameters.
core-dump	Configure a Cisco 1000 Series lightweight access point's memory core dump.
{enable | disable}	Enable or disable Ethernet-to-Ethernet bridging.
IP_address	IP Address for the TFTP server.
filename	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 1000 Series 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 delete

To delete a Foreign Access Point, use the **config ap delete** command.

config ap delete *MAC*

Syntax Description

config	Display configurations.
ap	Advanced parameters.
delete	Delete a Foreign Access Point.
MAC	Foreign Access Point MAC address.

Defaults

None.

Examples

```
> config ap delete 12:12:12:12:12:12
```

Related Commands

config ap

config ap disable

To disable a Cisco 1000 Series lightweight access point, use the **config ap disable** command.

config ap disable *Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
disable	Disable command.
Cisco_AP	Name of the Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config ap disable AP1
```

Related Commands

config ap enable

config ap enable

To enable a Cisco 1000 Series lightweight access point, use the **config ap enable** command.

config ap enable *Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
enable	Enable command.
Cisco_AP	Name of the Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config ap enable AP1
```

Related Commands

config ap disable

config ap crash-file clear-all

To delete all crash and radio core dump files, use the **config ap crash-file clear-all** command.

config ap crash-file clear-all

Syntax Description

config	Display configurations.
ap	Advanced parameters.
crash-file clear-all	Delete all crash and radio core dump files.

Defaults

None.

Examples

```
> config ap crash-file clear-all
```

Related Commands

config ap

config ap crash-file delete

To delete a single crash or radio core dump file, use the **config ap crash-file delete** command.

config ap crash-file delete *filename*

Syntax Description

config	Display configurations.
ap	Advanced parameters.
crash-file delete	Delete a single crash or radio core dump file.
filename	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 1000 Series 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 1000 Series lightweight access point.
crash-file get-crash-file	Collect the latest crash data for an access point.
Cisco_AP	Name of the Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config ap crash-file get-crash-file AP3
```

config ap crash-file get-radio-core-dump

To get a Cisco 1000 Series lightweight access point's radio core dump, use the **config ap crash-file get-radio-core-dump** command.

config ap crash-file get-radio-core-dump *Slot_ID Cisco_AP*

Syntax Description

config	Display configurations.
ap	Advanced parameters.
crash-file radio-core-dump	Get a Cisco 1000 Series lightweight access point's radio core dump.
Slot_ID	The slot ID (either 0 or 1).
Cisco_AP	Name of a Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config ap crash-file get-radio-core-dump 0 AP02
```

Related Commands

config ap

config ap group-name

To specify a descriptive group name for a Cisco 1000 Series lightweight access point, use the **config ap group-name** command. The Cisco 1000 Series lightweight access point must be disabled before changing this parameter.

config ap group-name *groupname Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
groupname	Descriptive group name.
Cisco_AP	Name of the Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config ap group-name superusers AP01
```

Related Commands

show ap summary

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*

Syntax Description

config	Display 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	Name of a Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config ap led-state enable AP02
```

Related Commands

config ap

config ap location

To modify the descriptive location of a Cisco 1000 Series lightweight access point, use the **config ap location** command. The Cisco 1000 Series lightweight access point must be disabled before changing this parameter.

config ap location *location Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
location	Descriptive location.
location	Location name (enclosed by double quotation marks).
Cisco_AP	Name of the Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config ap location "Building 1" AP1
```

Related Commands

show ap summary

config ap mode

Cisco Wireless LAN controllers communicate with Cisco 1000 Series lightweight access points in one of three modes: local (normal), reap (remote office, must connect to a Cisco 1030 remote edge lightweight access point), or monitor (listen-only). To change a Cisco Wireless LAN controller communication option for an individual Cisco 1000 Series lightweight access point, use the **config ap mode** command.

Note that the bridge mode can be set only on Cisco 1030 remote edge lightweight access points.

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 **rogure** to specify the rouge 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 1000 Series 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 1030 remote edge 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
```

Note The bridge mode can be set only on a Cisco 1030 remote edge lightweight access point.

Related Commands **show ap config**

config ap name

To modify the name of a Cisco 1000 Series lightweight access point, use the **config ap name** command.

config ap name *new_name old_name*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
name	Name of the Cisco 1000 Series lightweight access point.
new_name	Desired Cisco 1000 Series lightweight access point name.
old_name	Current Cisco 1000 Series lightweight access point name.

Defaults

None.

Examples

```
> config ap name AP1 AP2
```

Related Commands

show ap config

config ap port

To configure the port for a Foreign Access Point., use the **config ap port** command.

config ap port *MAC port*

Syntax Description

config	Display configurations.
ap	Advanced parameters.
port	Configure the port for a Foreign Access Point
MAC	Foreign Access Point MAC address.
port	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 pre-standard

To enable or disables the Inline Power Cisco Pre-Standard switch state for an access point, use the **config ap power pre-standard** command.

config ap power pre-standard {enable | disable} *Cisco_AP*

Syntax Description

config	Display 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 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config ap power pre-standard enable AP02
```

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 MAC*

Syntax Description

config	Display 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 1000 Series lightweight access point.
MAC	The switch port's MAC address to which the access point is connected.

Defaults

None.

Examples

```
> config ap power injector enable AP02 12:12:12:12:12:12
```

Related Commands

config ap

config ap primary-base

To set the Cisco 1000 Series lightweight access point primary Cisco Wireless LAN controller, use the **config ap primary-base** command. The Cisco 1000 Series 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*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
primary-base	Cisco 1000 Series lightweight access point primary Cisco Wireless LAN controller.
controller_name	Name of Cisco Wireless LAN controller.
Cisco_AP	Cisco 1000 Series lightweight access point name.

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 remote-debug

To enable or disable remote debugging of a Cisco 1000 Series lightweight access point or to remotely execute a command on a Cisco 1000 Series lightweight access point, use the **config ap remote-debug** command.

config ap remote-debug {enable | disable | exc-command *cmd***}** *Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
remote-debug	Cisco 1000 Series lightweight access point remote debug/remote command.
{enable | disable | exc-command *cmd***}**	Enable or disable remote debugging of a Cisco 1000 Series lightweight access point, or remotely execute a command.
cmd	Command to be executed.
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

Disabled.

Examples

To enable remote debugging on AP01:

```
> config ap remote-debug enable AP01
```

To disable remote debugging on AP02:

```
> config ap remote-debug disable AP02
```

To execute Cisco TAC-provided commands on AP03:

```
> config ap remote-debug exc-command (command) AP03
```

Related Commands

show sysinfo, **config sysname**

config ap reporting-period

To reset a Cisco 1000 Series lightweight access point, use the **config ap reset** command.

config ap reporting-period *period*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
reporting-period	Reporting-period command.
period	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 1000 Series lightweight access point, use the **config ap reset** command.

config ap reset *Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
reset	Reset command.
Cisco_AP	Cisco 1000 Series 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	Display 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 1000 Series 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	Display 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.
Cisco_AP	Name of the Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config ap rst-button enable AP03
```

Related Commands

config ap

config ap sniff 802.11a

To enable or disable sniffing on a Cisco 1000 Series lightweight access point radio, use the **config ap sniff 802.11a** command.

When the sniffer feature is enabled on a Cisco 1000 Series lightweight access point, it starts sniffing the signal on the given channel. It captures and forwards all the packets to the remote computer that runs airopeek, a packet analyzer for IEEE 802.11 wireless LANs. It includes information on timestamp, signal strength, packet size and so on.

Before a Cisco 1000 Series lightweight access point can act as a sniffer, a remote computer that runs Airopeek must be set up so that it can receive packets sent by the Cisco 1000 Series lightweight 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 802.11a {enable | disable} *channel ip_address Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
sniff	Sniffer command.
802.11a {enable | disable}	Enable or disable sniffing.
channel	Channel to be sniffed.
ip_address	The IP address of the sniffer server (remote Airopeek ip address)
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

None.

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 a Cisco 1000 Series lightweight access point radio, use the **config ap sniff 802.11b** command.

When the sniffer feature is enabled on a Cisco 1000 Series lightweight access point, it starts sniffing the signal on the given channel. It captures and forwards all the packets to the remote computer that runs airopeek (a packet analyzer for IEEE 802.11 wireless LANs). It includes information on timestamp, signal strength, packet size and so on.

Before a Cisco 1000 Series lightweight access point can act as a sniffer, a remote computer that runs Airopeek must be set up so that it can receive packets sent by the Cisco 1000 Series lightweight 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 | disable} *channel ip_address Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
sniff 802.11b	Sniffer command.
{enable | disable}	Enable or disable sniffing.
channel	Channel to be sniffed.
ip_address	IP address of the sniffer server (remote Airopeek ip address).
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

None.

Examples

```
> config ap sniff 80211b enable 23 11.22.44.55 AP01
```

Related Commands

show ap config, **config ap sniff 802.11a**

config ap stats-timer

Use this command to set the time in seconds that the Cisco 1000 Series lightweight access point sends its DOT11 statistics to the Cisco Wireless LAN controller. A value of 0 (zero) means the Cisco 1000 Series lightweight access point will not send any DOT11 statistics. The acceptable range for the timer is from 0 to 65535 seconds, and the Cisco 1000 Series lightweight access point must be disabled to set this value.

config ap stats-timer *period Cisco_AP*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
stats-timer	Cisco 1000 Series lightweight access point primary Cisco Wireless LAN controller.
period	Time in seconds from 0 to 65535. A zero value disables the timer.
Cisco_AP	Cisco 1000 Series lightweight access point name.

Defaults

0 (disabled).

Examples

```
> config ap stats-timer 600 AP2
```

Related Commands

config ap disable

config ap secondary-base

To set the Cisco 1000 Series lightweight access point secondary Cisco Wireless LAN controller, use the **config ap secondary-base** command. The Cisco 1000 Series 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*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
primary-base	Cisco 1000 Series lightweight access point secondary Cisco Wireless LAN controller.
controller_name	Name of Cisco Wireless LAN controller.
Cisco_AP	Cisco 1000 Series lightweight access point name.

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 static-ip

To configure Cisco 1000 Series lightweight access point static IP address settings, use the **config ap static-ip** command.

config ap static-ip {enable | disable} *Cisco_AP ip_address net_mask gateway*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
static-ip	configure Cisco 1000 Series lightweight access point static IP address settings.
{enable | disable}	Configure the Cisco 1000 Series lightweight access point static IP address. Disable the Cisco 1000 Series lightweight access point static IP address. The Cisco 1000 Series lightweight access point uses DHCP to get the IP address.
Cisco_AP	Cisco 1000 Series lightweight access point name.
ip_address	Cisco 1000 Series lightweight access point IP address
net_mask	The Cisco 1000 Series lightweight access point network mask.
gateway	IP address of the Cisco 1000 Series 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 tertiary-base

To set the Cisco 1000 Series lightweight access point tertiary Cisco Wireless LAN controller, use the **config ap tertiary-base** command. The Cisco 1000 Series 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*

Syntax Description

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
tertiary-base	Cisco 1000 Series lightweight access point tertiary Cisco Wireless LAN controller.
controller_name	Name of Cisco Wireless LAN controller.
Cisco_AP	Cisco 1000 Series lightweight access point name.

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

To initiate access point image downgrade from a TFTP server, use the **config ap tftp-downgrade** command.

config ap tftp-downgrade *IP_address filename Cisco_AP*

Syntax Description

config	Display configurations.
ap	Advanced parameters.
tftp-downgrade	Initiate access point image downgrade from a TFTP server.
IP_address	static IP address of the specified Cisco 1000 Series lightweight access point.
filename	Image file name on the TFTP server.
Cisco_AP	Name of the Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config ap tftp-downgrade 192.1.1.1 img1 AP02
```

Related Commands

config ap

config ap wlan

To enable or disable Wireless LAN override for a Cisco 1000 Series lightweight access point radio, and to add or delete Wireless LANs to or from a Cisco 1000 Series 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 1000 Series lightweight access point.
wlan	Reset command.
{add | delete | enable | disable}	• Add or delete a Wireless LAN on an access point. (Cisco 1000 Series 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.
wlan_id	Optional Cisco Wireless LAN controller ID assigned to a Wireless LAN.
Cisco_AP	Cisco 1000 Series 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 wlandisable 802.11a AP03
```

Related Commands

show ap wlan

config exclusionlist

To create or delete an Exclusion List entry, use the **config exclusionlist** command.

config exclusionlist {add | delete | 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	The description, up to 32 characters, for an excluded entry.

Defaults

None.

Examples

```
> config exclusionlist add 0:0b:85:01:18:b0 lab

> config exclusionlist delete 0:0b:85:01:18:b0 lab
```

Related Commands

show exclusionlist

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 certificate

To configures 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 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 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.
MAC	Client MAC address.

Defaults

None.

Examples

```
> config client deauthenticate 11:11:11:11:11:11
```

Related Commands

show client summary, **show client detail**

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.
country_code	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 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 *URL*	Set the redirect URL to the specified address.

Defaults

None.

Examples

```
> config custom-web redirectUrl abc.com
```

Related Commands

config custom-web weblogo, config custom-web webmessage, config custom-web webtitle, config custom-web ext-webauth-mode, config custom-web ext-webauth-url, config custom-web ext-webserver, 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, config custom-web ext-webserver, 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 *message*	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, config custom-web ext-webserver, 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 *title*	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, config custom-web ext-webserver, show custom-web

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, config custom-web ext-webserver, 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 *URL*	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, config custom-web ext-webserver, 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 | delete} *index IP_address*

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.
index	Index of the external web server in the list of external web server. Must be a number between 1 and 20.
IP_address	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 database

To configure the local database, use the **config database** command. Use the show database command to display local database configuration.

config database *size*

Syntax Description

config database	Command action.
size	A database size between 512 and 2040

Defaults

None.

Examples

Configures the dhcp lease for scope 003.

```
> config database 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* **| 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 *scope start end*	Configure an address range to allocate. You must specify the scope name and the first and last addresses of the address range.
create-scope *name*	Create a new dhcp scope. You must specify the scope name.
default-router *scope*	Configure the default routers for the specified scope.
delete-scope *scope*	Delete the specified DHCP scope.
disable *scope*	Disable the specified DHCP scope.
dns-servers *scope dns1* **[***dns2***] [***dns3***]**	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 *scope domain*	Configure the DNS domain name. You must specify the scope and domain names.
enable *scope*	Enable the specified dhcp scope.
lease *scope lease_duration*	Configure the lease duration (in seconds) for the specified scope.
netbios-name-server *scope wins1* **[***wins2***] [***wins3***]**	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 *scope network netmask*	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 known ap

To configure a known Cisco 1000 Series 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 1000 Series 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 1000 Series lightweight access point.

Defaults

None.

Examples

```
> config known ap add ac:10:02:72:2f:bf 12
```

Related Commands

config ap

CONFIG INTERFACE COMMANDS

Use the config interface commands to configure interface commands.

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 2000 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 4100 Series Wireless LAN controllers and 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 an interface's address information, 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 IP_address netmask gateway***}**

Syntax Description

config interface address	Command action.
ap-manager *IP_address netmask gateway*	Configures the access point manager interface. You must specify the IP address, network mask, and gateway information.
management *IP_address netmask gateway*	Configures the management interface. You must specify the IP address, network mask, and gateway information.
service-port *IP_address netmask*	Configures the out-of-band service Port for the interface. You must specify the IP address of the interface and its network mask.
virtual *IP_address*	Configures the virtual gateway interface. You must specify the IP address of the interface.
interface-name IP_address netmask gateway	Configures the specified interface name. You must specify the interface's IP address, network mask, and gateway information.

Defaults

None.

Examples

```
> config interface address ap-manger 172.168.2.3 255.255.0.0 172.168.2.1
```

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 add a new dynamic interface, 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.
interface_name	Interface's name.
vlan-id	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.
interface-name	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 *server1* **[***server2***] |**
management *server1* **[***server2***] | service-port {enable | disable} |**
interface-name server1 **[***server2***]}**

Syntax Description

config interface dhcp	Command action.
ap-manager *server1* **[***server2***]**	Configures the access point manager interface. You must enter the address of the primary DHCP server. Optionally, you can also enter the address of the alternate DHCP server.
management *server1* **[***server2***]**	Configures the management interface. You must enter the address of the primary DHCP server. Optionally, you can also enter the address of the alternate DHCP server.
service-port {enable | disable}	Enables or disables DHCP for the out-of-band service port.
interface-name server1 **[***server2***]**	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 service-port DHCP02
```

Related Commands

show interface

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 *DNS_host*	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 assign an interface to a physical port, use the **config interface port** command.

config interface port {ap-manager | management | *interface_name***}** *port1* **[***port2***]**

Syntax Description

config interface port	Command action.
ap-manager	Configures the access point management interface to the specified port number.
management	The management interface.
vlan-intf-name	VLAN or interface name
port1 **[***port2***]**	Interface's physical port number.

Defaults

None.

Examples

```
> config interface port management 3
```

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

Request failed - Active WLAN using interface. Disable WLAN first.
```

Related Commands

show interface

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 location add

To create a new Cisco 1000 Series lightweight access point location, use the **config location add** command.

config location add *location* **[***description***]**

Syntax Description

config	Configure parameters.
location	Cisco 1000 Series lightweight access point location.
add	Add a location.
location	Location name.
[*description***]**	(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 1000 Series lightweight access point location, use the **config location delete** command.

config location delete *location*

Syntax Description

config	Configure parameters.
location	Cisco 1000 Series lightweight access point location.
delete	Delete a location.
location	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 1000 Series lightweight access point location, use the **config location description** command.

config location description *location_name description*

Syntax Description

config	Configure parameters.
location	Cisco 1000 Series lightweight access point location.
description	Description of a location.
location_name	Location name.
description	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 enable or disable Cisco 1000 Series lightweight access point location-based overrides, use the **config location disable** command.

config location disable

Syntax Description

config	Configure parameters.
location	Cisco 1000 Series 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 1000 Series lightweight access point location-based overrides, use the **config location enable** command.

config location enable

Syntax Description

config	Configure parameters.
location	Cisco 1000 Series 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 1000 Series 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 1000 Series 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 loginsession

To manage user connections to the switch, use the **config loginsession** 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 location interface-mapping add warehouse 13
```

Related Commands **show location**, **config location add**, **config location delete**, **config location description**, **config location**

CONFIG 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 wlan_id interface_name description*

Syntax Description

config	Configure parameters.
macfilter	Local MAC address filter.
add	Creates a local MAC filter entry.
MAC	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	Short description of the interface (up to 32 characters).

Defaults

None.

Examples

```
> config macfilter add 11:11:11:11:11:11 1 lab02 labconnect
```

Related Commands

show macfilter

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.
MAC	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.
MAC	Client MAC address.
interface	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 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.
MAC	Client MAC address
wlan_id	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**

CONFIG MGMTUSER 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.
{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.
username	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 delete** command.

config mgmtuser description *username description*

Syntax Description

config	Configure parameters.
mgmtuser	Management user account.
description	Delete a management user account.
username	Account username. Up to 24 alphanumeric characters.
description	Description of the account. Up to 32 alphanumeric characters within double quotes.

Defaults

None.

Examples

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

Related Commands

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
username	Account username. Up to 24 alphanumeric characters.
password	Account password. Up to 24 alphanumeric characters.

Defaults None.

Examples

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

Related Commands **show mgmtuser**

CONFIG MOBILITY COMMANDS

Use the config mobility commands to configure mobility settings.

config mobility group anchor

To configures the mobility Wireless LAN anchor list, use the **config mobility group anchor** command.

config mobility group anchor {add | delete} *wlan_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.
IP_address	Member switch IP address to anchor Wireless LAN.

Defaults

None.

Examples

```
> config mobility group anchor add 2 192.12.1.5
```

Related Commands

show mobility, config mobility group domain, config mobility group member

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.
domain_name	Domain name. Up to 31 characters; case sensitive.

Defaults

None.

Examples

```
> config mobility group domain lab1
```

Related Commands

show mobility, config mobility group anchor, config mobility group member

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	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, config mobility group anchor, config mobility group domain

config mobility secure-mode

To configure the secure mode for mobility messages between Cisco Wireless LAN controllers/appliances, 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

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**

CONFIG MSGLOG LEVEL COMMANDS

Use the msglog level 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 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

```
> config msglog level warning

> show msglog

Message Log Severity Level..................... WARNING
(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 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 2000 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 4100 Series Wireless LAN controllers and 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 *acl-name* 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.
index	NAC server index number.
IP_address	NAC server IP address.
port	NAC server UDP port number.
secret	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.
index	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.
index	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.
index	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**

CONFIG NETUSER COMMANDS

Use the config netuser commands to configure netuser settings.

config netuser add

To add a user to the local network, use the **config netuser add** command.

config netuser add *username password wlan_id* **[***description***]**

Syntax Description

config	Configure parameters.
netuser	Local network user.
add	Add a user.
username	Network username. Up to 24 alphanumeric characters.
password	User password. Up to 24 alphanumeric characters.
wlan_id	Wireless LAN Identifier assigned to the user. A zero value associates the user with any Wireless LAN.
[*description***]**	Short optional description. Up to 32 characters enclosed in double-quotes.

Defaults

None.

Examples

```
> config netuser add able1 able1 1
```

Related Commands

show netuser

config netuser delete

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

config netuser delete *username*

Syntax Description

config	Configure parameters.
netuser	Local network user.
delete	Delete a user.
username	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.
username	Network username.
description	Optional user description. Up to 32 alphanumeric characters enclosed in double quotes.

Defaults

None.

Examples

```
> config netuser description able1 "HQ1 Contact"
```

Related Commands

show netuser

config netuser maxUserLogin

To configure the maximum number of login sessions allowed for a network user, use the **config netuser maxUserLogin** command.

config netuser maxUserLogin *count*

Syntax Description

config	Configure parameters.
netuser	Local network user.
maxUserLogin	Configure the maximum number of login sessions allowed for a network user.
count	Maximum number of login sessions for a single user. The allowed values are from 0 (unlimited) to 8.

Defaults

0 (unlimited).

Examples

```
> config netuser 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.
username	Network username. Up to 24 alphanumeric characters.
password	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**

CONFIG NETWORK COMMANDS

Use the config network commands to configure network settings.

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

config network ap-fallback

To configure Cisco 1000 Series 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 1000 Series lightweight access point fallback.
{enable | disable}	Enable or disable Cisco 1000 Series lightweight access point fallback.

Defaults

Enabled.

Examples

```
> config network ap-fallback enable
```

Related Commands

show network

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

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.
seconds	Timeout in seconds. Minimum value is 10. Default value is 300.

Defaults

300

Examples

```
> config network arptimeout 240
```

Related Commands

show network

config network arpunicast

To set the ARP proxy ARP mode, use the **config network arpunicast** command.

config network arpunicast {enable | disable}

Syntax Description

config	Configure parameters.
network	Cisco Wireless LAN controller network parameter.
arpunicast	Set the ARP proxy ARP mode.
{enable | disable}	• Enter **enable** to enable unicast ARP translation. • Enter **disable** to use standard proxy ARP.

Defaults

None.

Examples

```
> config network arpunicast enable
```

Related Commands

show network

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-config 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.
shared_secret	Bridging shared secret string. Up to ten bytes.

Defaults

Enabled.

Examples

```
> config network bridging-shared-secret shhh2
```

Related Commands

show network

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.

SSID is a code attached to all packets on a wireless network to identify each packet as part of that network.

Each client is connected to a particular Wireless LAN (through a Cisco 1000 Series lightweight access point) identified by the SSID. If the client moves out of reach of the connected Cisco 1000 Series lightweight access point, the client has to reconnect to the Cisco Wireless LAN controller using a different Cisco 1000 Series lightweight access point. This procedure consumes some time as the DHCP (Dynamic Host Configuration Protocol) Server has to assign an IP Address to the client.

When the Fast SSID option is enabled, the Cisco Wireless LAN controller uses the existing IP Address of the client even if the client is on a different Wireless LAN.

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.

Examples

```
> config network fast-ssid-change enable
```

Related Commands

show network

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}	Enables or disables a Cisco Wireless LAN controller acting as a Cisco 1000 Series 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 1000 Series 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

config network multicast

To enable or disable the Cisco Wireless LAN controller multicast support, use the **config network multicast** command.

config network multicast {enable | disable}

Syntax Description

config	Configure parameters.
network	Network parameters.
multicast	Configure multicast support.
{enable | disable}	Enable or disable the Cisco Wireless LAN controller multicast support.

Defaults

Disabled.

Examples

```
> config network multicast enable
```

Related Commands

show network

config network otap-mode

To enable or disable over-the-air provisioning (OTAP) of Cisco 1000 Series 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

config network peer-blocking

To configure the peer-to-peer blocking feature, use the **config network peer-blocking** command.

config network peer-blocking {enable | disable}

Syntax Description

config	Configure parameters.
network	Network parameters.
peer-blocking	Configure peer-to-peer blocking.
{enable | disable}	• Enter **enable** to force same-subnet clients to communicate through a higher-level router. • Enter **disable** to allow same-subnet clients to communicate through the Cisco Wireless LAN controller.

Defaults

Disabled.

Examples

```
> config network peer-blocking enable
```

Related Commands

show network

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.
name	RF-Network name. Up to 19 characters.

Defaults

None.

Examples

```
> config network rf-network-name travelers
```

Related Commands

show network

config network secureweb

To change the state of the secure web (https = http + SSL) interface, use the **config network secureweb** command.

config network secureweb {enable | disable}

Syntax Description

config	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

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

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

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.
seconds	Timeout duration in seconds. Minimum value is 10. Default value is 300.

Defaults

300

Examples

```
> config network usertimeout 1200
```

Related Commands

show network

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.
port	Port number.

Defaults

None.

Examples

```
> config network web-auth-port 1200
```

Related Commands

show network

config network webmode

To enable or disable the web interface, 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

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

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

CONFIG 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 | *port***}**	• Enter **all** to configure all ports. • Enter the number of the port to configure.
{enable | disable}	Enable or disable the specified ports.

Defaults

Enabled.

Examples

To disable port 8:

```
> config port adminmode 8 disable
```

To enable all ports:

```
> config port adminmode all enable
```

Related Commands

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 | *port***}**	• Enter **all** to configure all ports. • Enter the number of the port to configure.
{enable | disable}	Enable or disable the specified ports.

Defaults

Enabled.

Examples

To disable port 8 traps:

```
> config port linktrap 8 disable
```

To enable all port traps:

```
> config port linktrap all enable
```

Related Commands

show port

config port multicast

To change the multicast appliance service for a single port or all Cisco Wireless LAN controller ports, use the **config port multicast** 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:

```
> config port multicast appliance 3 enable
```

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.
prompt	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 queue_length

To configure the Quality of Service parameter, use the **config qos** command.

config qos queue_length {bronze | silver | gold | platinum} *length*

Syntax Description

config qos	Command action.
queue_length	Configure QoS queue length.
{bronze | silver | gold | platinum}	Enter one of the four supported queue names.
length	Queue length (10 to 255).

Defaults None.

Examples

```
> config qos queue_length gold 12
```

Related Commands **show qos queue_length all**

CONFIG RADIUS ACCT 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.
index	RADIUS server index. Cisco Wireless LAN controller begins search with 1.
ip_address	RADIUS server's IP address.
port	RADIUS server's UDP port number for the interface protocols.
{ascii | hex}	RADIUS server's secret type: **ascii** or **hex**.
secret	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.
index	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.
index	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.
index	RADIUS server index.

Defaults

None.

Examples

```
> config radius acct enable 1
```

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.
index	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.
index	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.
index	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}

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	RADIUS server index.

Defaults

None.

Examples

```
> config radius acct ipsec encryption 3des 3
```

Related Commands

show radius acct statistics

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.
index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Defaults

None.

Examples

```
> config radius acct retransmit-timeout 5
```

Related Commands

show radius acct statistics

CONFIG RADIUS AUTH COMMANDS

Use the config radius acct 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.
index	RADIUS server index. Cisco Wireless LAN controller begins search with 1.
ip_address	RADIUS server's IP address.
port	RADIUS server's UDP port number for the interface protocols.
{ascii | hex}	RADIUS server's secret type: **ascii** or **hex**.
secret	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.
index	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.
index	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.
index	RADIUS server index.

Defaults

None.

Examples

```
> config radius auth enable 1
```

Related Commands

show radius auth statistics

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.
index	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 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 disable *index*

Syntax Description

config	Configure parameters.
radius auth	RADIUS authentication server.
ipsec disable	Disable IPSec support for an authentication server.
index	RADIUS server index.

Defaults

None.

Examples

```
> config radius auth ipsec disable 1
```

Related Commands

show radius acct statistics

config radius auth ipsec enable

To configure IPSec support for an authentication server for the Cisco Wireless LAN controller, use the **config radius auth ipsec enable** command.

config radius auth ipsec enable *index*

Syntax Description

config	Configure parameters.
radius auth	RADIUS authentication server.
ipsec enable	Enable IPSec support for an authentication server.
index	RADIUS server index.

Defaults

None.

Examples

```
> config radius auth ipsec enable 1
```

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 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 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.
index	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 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.
index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Defaults

None.

Examples

```
> config radius auth retransmit-timeout 5
```

Related Commands

show radius auth statistics

config radius 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 callStationIdType	Configure callStationIdType information.
{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	Display configurations.
rfid timeout	Configure the static RFID tag data timeout.
seconds	Timeout in seconds (from 60 to 7200).

Defaults

None.

Examples

```
> config rfid timeout 60
```

Related Commands

show rfid summary, **config rfid statistics.**

config rogue ap

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

config rogue ap {acknowledged | alert | contain | known} *MAC*

Syntax Description

config	Configure parameters.
rogue ap	Rogue access point status.
{acknowledged | alert | contain | known}	• 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.
MAC	MAC address of the rogue access point.

Defaults

None.

Examples

```
> config rogue ap acknowledge 11:11:11:11:11:11
```

Related Commands

show rogue ap summary, **show rogue ap detailed**

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 | alert | contain} *MAC*

Syntax Description

config	Configure parameters.
rogue adhoc	Ad hoc rogue access point.
{acknowledged | alert | contain}	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.
MAC	MAC address of the ad hoc rogue access point.

Defaults

None.

Examples

```
> config rogue adhoc acknowledge 11:11:11:11:11:11
```

Related Commands

show rogue adhoc summary, **show rogue adhoc detailed**, **config adhoc rogue**

config rogue client

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

config rogue client {alert | contain} *MAC*

Syntax Description

config	Configure parameters.
rogue client	Rogue client status.
{alert | contain}	• Enter **alert** to configure the rogue client to the alarm state. • Enter **contain** to start containing a rogue client.
MAC	MAC address of the rogue client.

Defaults None.

Examples

```
> config rogue client acknowledge 11:11:11:11:11:11 5
```

Related Commands **show rogue client summary**, **show rogue client detailed**, **config rogue client**

CONFIG ROUTE COMMANDS

Use the config route commands to configure network route settings.

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.
ip_address	Network IP Address.
netmask	The subnet mask for the network.
gateway	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.
ip_address	Network IP Address.

Defaults None.

Examples

```
> config route delete 10.1.1.0
```

Related Commands **show route all**, **config route add**

CONFIG 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 | 115200}

Syntax Description

config	Configure parameters.
serial	Configure serial port baud rate.
{1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}	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.
minutes	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 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
timeout	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**

CONFIG 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.
name	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.
name	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.
ip_address	SNMP community IP address.
ip_mask	SNMP community subnet mask.
name	SNMP community name.

Defaults

None.

Examples

```
> config snmp community ipaddr 10.10.10.10.2 255.255.255.0 public
```

Related Commands

show snmp community, **config snmp community mode**, **config snmp community accessmode**, **config snmp community create**, **config snmp community delete**, **config snmp community ipaddr**

config snmp community mode

To enable or disable an SNMP community, use the **config snmp community mode** command.

config snmp community mode {enable | disable} *name*

Syntax Description

config snmp community	Configure SNMP community parameters.
mode	Configure an SNMP community
{enable | disable}	Enable or disable the community.
name	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.
contact	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.
location	SNMP system location name. Up to 31 alphanumeric characters.

Defaults None.

Examples

```
> config snmp syslocation Building_2a
```

Related Commands **show snmpcommunity**

CONFIG SNMP TRAPRECEIVER COMMANDS

Use the config snmp 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.
name	SNMP community name. Up to 16 characters.
ip_address	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.
name	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

CONFIG SNMP V3USER 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} [***auth_key***] [***encrypt_key***]**

Syntax Description

config	Configure parameters.
snmp	SNMP parameters.
v3user create	Create a version 3 SNMP.
username	Version 3 SNMP username.
{ro | rw}	• Enter **ro** to specify a Read Only user privileges. • Enter **rw** to specify a Read/Write user privileges.
{none | hmacmd5 | hmacsha}	Enter an authentication protocol for a v3 user or **none** if no authentication is required.
{none | des}	• Enter **none** if no encryption is required. • Enter **des** to use the des encryption protocol.
[*auth_key***]**	Authentication key for the hmacmd5 or hmacsha authentication protocol.
[*encrypt_key***]**	Encryption key for the des encryption protocol.

Defaults

SNMP v3 User Name AccessMode Authentication Encryption

--- --- --- ---

default Read/Write HMAC-MD5 CBC-DES

Examples

To add an SNMP username test with read-only privileges and no encryption or authentication:

```
> config snmp v3user create test ro none none
```

Related Commands

show snmp v3user

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.
username	Username to delete.

Defaults

SNMP v3 User Name AccessMode Authentication Encryption

---------- ---------- ---------- ----------

default Read/Write HMAC-MD5 CBC-DES

Examples

This will remove an SNMP user named test.

```
> config snmp v3user delete test
```

Related Commands

show snmp v3user

config snmp version

To enable or disable selected SNMP versions, use the **config snmp version** command.

config snmp version {v1 | v2 | v3} {enable | disable}

Syntax Description

config	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

CONFIG SPANNINGTREE 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.
{*cost* **| auto}**	Enter cost in decimal as determined by the network planner or **auto** (default cost).
{*port* **| 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.
priority_num	Enter a priority number from 0 to 255.
port	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**

CONFIG SPANNINGTREE SWITCH COMMANDS

Use the config spanningtree switch commands to configure spanningtree 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.
priority_num	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.
seconds	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.
seconds	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.
seconds	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**

CONFIG SWITCHCONFIG 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}

Note The 2000 series controllers do not support Layer 2 LWAPP.

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 syslog

To send or disable sending system logs, use the **config syslog** command.

config syslog {*ip_address* **| disable}**

Syntax Description

config	Configure parameters.
syslog	Configure system logs.
{*ip_address* **| disable}**	• Enter an IP address to send logs to. • Enter **disable** to disable system logs.

Defaults

Disable

Examples

```
> config syslog 10.1.1.1
Sending logs to 10.1.1.1
> config syslog disable
Syslog disabled.
```

Related Commands

show syslog

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.
name	System name. Up to 31 alphanumeric characters.

Defaults

None.

Examples

```
> config sysname Ent_01
```

Related Commands

show sysinfo

config time manual

To set the system time, use the **config time manual** command.

config time manual *MM/DD/YY HH:MM:SS*

Syntax Description

config	Command action.
time	Configures system time or servers.
manual	Configures the system time.
MM/DD/YY	Enter date.
HH:MM:SS	Enter time.

Defaults

None.

Examples

```
> config time manual 02/11/2003 15:29:00
```

Related Commands

show time

config time ntp

To set the Network Time Protocol, use the **config time ntp** command.

config time ntp {interval *seconds* **| server** *index ip_address***}**

Syntax Description

config	Command action.
time	Configures system time or servers.
ntp	Configures the Network Time Protocol.
interval	
{interval | server}	• Enter interval to configure the Network Time Protocol polling interval. • Enter server to configure the Network Time Protocol servers.
seconds	NTP polling interval in seconds (between 6800 and 604800).
index	NTP server index.
ip_address	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 configures 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.
delta_hours	Enter the local hour difference from Universal Coordinated Time (UCT).
delta_mins	Enter the local minute difference from UCT.

Defaults

None.

Examples

```
> config time timezone enable 2 0
```

Related Commands

show time

CONFIG TRAPFLAGS COMMANDS

Use the config trapflags commands to configure trapflags 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 1000 Series 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 1000 Series lightweight access point traps flag.
{register | interfaceUp}	• Enter **register** to enable sending trap when a Cisco 1000 Series lightweight access point registers with Cisco switch. • Enter **interfaceUp** to enable sending trap when a Cisco 1000 Series 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-disassocate | 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-disassocate | 802.11-deauthenticate | 802.11-authfail | 802.11-assocfail | excluded}	• Enter **802.11-disassocate** 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 1000 Series lightweight access point interface. • Enter **channel** to enable trap sending when RF manager automatically changes channel for the Cisco 1000 Series lightweight access point interface. • Enter **antenna** to enable trap sending when RF manager automatically changes antenna for the Cisco 1000 Series 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**

CONFIG WATCHLIST COMMANDS

Use the config watchlist commands to configure watchlist settings.

config watchlist add

To add a watchlist entry for a wireless LAN, use the **config watchlist add** command.

config watchlist add {mac *MAC* | **username** *username***}**

Syntax Description

config watchlist	Command action.
add	Add a watchlist entry.
{mac *MAC* | **username** *username***}**	• Enter mac and specify the MAC address of the wireless LAN. • 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* | **username** *username***}**	• Enter mac and specify the MAC address of the wireless LAN to delete from the list. • Enter username and specify the name of the user to delete from the list.

Defaults

None.

Examples

```
> config watchlist delete mac a5:6b:ac:10:01:6b
```

Related Commands

config watchlist add, **config watchlist enable, config watchlist disable**, **show watchlist**

config watchlist disable

To disable the client watchlist, use the **config watchlist disable** command.

config watchlist disable

Syntax Description

config	Command action.
watchlist	Configure the client watchlist.
disable	Disable the client watchlist.

Defaults

None.

Examples

```
> config watchlist disable
```

Related Commands

config watchlist add, **config watchlist delete**, **show watchlist**

config watchlist enable

To enable a watchlist entry for a wireless LAN, use the **config watchlist enable** command.

config watchlist enable

Syntax Description

config watchlist	Command action.
watchlist	Configure the client watchlist.
enable	Enable the client watchlist.

Defaults None.

Examples

```
> config watchlist enable
```

Related Commands **config watchlist add**, **config watchlist delete**, **show watchlist**

CONFIG 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.

config wlan 7920-support {ap-cac-limit | client-cac-limit} {enable | disable} *wlan_id*

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.
wlan_id	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 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, DSCP, 802.1p priority tag values and ACL provided by the AAA server, as long as they are predefined in the Cisco Wireless LAN controller interface configuration. (This VLAN switching by AAA override is also referred to as Identity Networking.)

For instance, if the Corporate Wireless LAN primarily uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the Operating System redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.

When AAA override is disabled, all client authentication defaults to the Cisco Wireless LAN controller authentication parameter settings, and authentication is only performed by the AAA server if the Cisco Wireless LAN controller Wireless LAN do not contain any client-specific authentication parameters.

The AAA override values may come from a RADIUS server, for example.

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 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 exclusionlist

To configure exclusion list (blacklist) timeout for a wireless LAN, use the **config wlan exclusionlist** command.

Set the timeout in seconds for an automatically disabled client. Client machines are disabled by MAC address. A timeout setting of 0 indicates that the client is permanently disabled and that administrative control is required to remove the client from the automatic disable.

config wlan exclusionlist {*wlan_id* **| foreignAp} {enabled | disabled |** *seconds***}**

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
exclusionlist	Configure exclusion list timeout.
{*wlan_id* **| foreignAp}**	• Enter a Wireless LAN identifier between 1 and 16. • Enter **foreignAp** for third party access points.
{enabled | disabled | *seconds***}**	• Enter **enabled** to enable exclusion-listing. • Enter **disabled** to disable exclusion-listing. • Enter the exclusion-list timeout in seconds. A zero value requires administrator override.

Defaults

Not enabled

Examples

```
> config wlan exclusionlist 1 3
```

```
> config wlan exclusionlist 1 disabled
```

Related Commands

show exclusionlist

config wlan create

To create a wireless LAN, use the **config wlan create** command.

config wlan create {*wlan_id wlan_name* **| foreignAp}**

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
create	Create a Wireless LAN.
{*wlan_id wlan_name* **| foreignAp}**	• Enter a 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.

Defaults

None.

Examples

```
> config wlan create 1 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.
{*wlan_id* | **foreignAp}**	• Enter a Wireless LAN identifier between 1 and 16. • Enter **foreignAp** for third party access points.
ip_address	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 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.
{*wlan_id* | **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 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.
{*wlan_id* | **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 interface

To associate a wireless LAN with an existing interface, use the **config wlan interface** command.

config wlan interface {*wlan_id* | **foreignAp}** *interface-name*

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
interface	Configure the Wireless LAN's interface.
{*wlan_id* | **foreignAp}**	• Enter a Wireless LAN identifier between 1 and 16. • Enter **foreignAp** for third party access points.
interface-name	Existing 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 of 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 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.
wlan_id	Enter a Wireless LAN identifier between 1 and 16.
ip_address	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 qos

To change the quality of service for a wireless LAN, use the **config wlan qos** command.

config wlan qos {*wlan_id* | **foreignAp} {bronze | silver | gold | platinum}**

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
qos	Quality of service.
{*wlan_id* | **foreignAp}**	• Enter a Wireless LAN identifier between 1 and 16. • Enter **foreignAp** for third party access points.
{bronze | silver | gold | platinum}	Enter QoS policy: **bronze**, **silver**, **gold**, or **platinum**.

Defaults

None.

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.
wlan_id	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} {add *wlan_id server_id* **| delete** *wlan_id* **{all |** *server_id***}}**

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
radius-server	RADIUS servers.
{auth | acct}	Configures a RADIUS authentication or accounting server.
{add | delete}	Add or delete a link to a configured RADIUS Server.
wlan_id	Wireless LAN identifier between 1 and 16.
server_id	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**

config wlan wmm

To configure WMM (WME), use the **config wlan wmm** command.

config wlan wmm {allow | disable | require} *wlan_id*

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
wmm	Configure WMM.
{allow | disable | require}	• Enter **allow** to allow WMM on the Wireless LAN. • Enter **disable** to disable WMM on the Wireless LAN. • Enter **require** to require WMM-enabled clients on the Wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 16.

Defaults

None.

Examples

```
> config wlan wmm allow 1
```

Related Commands

show trapflags

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 Wireless LAN SECURITY COMMANDS

Use the 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 | disable | encryption} {*wlan_id* | **foreignAp} [0 | 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 cranite

To change the state of the Cranite passthrough, use the **config wlan security cranite** command.

config wlan security cranite {enable | disable} {*wlan_id* | **foreignAp}**

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the Wireless LAN security policy.
cranite	Configure Cranite passthrough.
{enable | disable}	Enable or disable cranite passthrough.
{*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 cranite enable 16
```

Related Commands

show wlan

config wlan security fortress

To change the state of the Fortress passthrough, use the **config wlan security fortress** command.

config wlan security fortress {enable | disable} {*wlan_id* | **foreignAp}**

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the Wireless LAN security policy.
fortress	Configure Fortress passthrough.
{enable | disable}	Enable or disable Fortress passthrough.
{*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 fortress enable 16
```

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.
{*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 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.
ip_address	quote-of-the-day server IP for cfg-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 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 | pre-share-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.
{*wlan_id* | **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 ipsec enable 3 192.12.1.1
```

Related Commands

show wlan

config wlan security l2tp authentication

To configure the l2tp IPSec authentication transform used on the wireless LAN, use the **config wlan security l2tp authentication** command.

config wlan security l2tp authentication {hmac-md5 | hmac-sha-1} *wlan_id*

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the Wireless LAN security policy.
l2tp	L2tp.
authentication |	IPSec authentication transform (hmac-md5 or hmac-sha-1).
{hmac-md5 | hmac-sha-1}	Enter the IPSec HMAC-MD5 or IPSec HMAC-SHA-1 authentication protocol.
wlan_id	A Wireless LAN identifier between 1 and 16.

Defaults

None.

Examples

```
> config wlan security l2tp authentication hmac-sha-1 3
```

Related Commands

show wlan

config wlan security l2tp disable

To disable l2tp used on the wireless LAN, use the **config wlan security l2tp disable** command.

config wlan security l2tp disable *wlan_id*

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the Wireless LAN security policy.
l2tp	Configure L2tp.
disable	Disable L2TP.
wlan_id	A Wireless LAN identifier between 1 and 16.

Defaults

None.

Examples

```
> config wlan security l2tp disable 1
```

Related Commands

show wlan

config wlan security l2tp enable

To configure l2tp used on the wireless LAN, use the **config wlan security l2tp enable** command.

config wlan security l2tp enable *wlan_id*

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the Wireless LAN security policy.
l2tp	Configure L2tp.
enable	Enable L2TP.
wlan_id	A Wireless LAN identifier between 1 and 16.

Defaults

None.

Examples

```
> config wlan security l2tp enable 1
```

Related Commands

show wlan

config wlan security l2tp encryption

To configure IPSec encryption transform used on the wireless LAN, use the **config wlan security l2tp encryption** command.

config wlan security l2tp encryption {3des | aes | des} *wlan_id*

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the Wireless LAN security policy.
l2tp	Configure L2tp.
encryption |	Configure IPSec configuration transform (3des, aes, or des).
{3des | aes | des}	• Enter **3des** to enable IPSec 3DES Encryption. • Enter **aes** to enable IPSec AES Encryption. • Enter **des** to enable IPSec DES Encryption.
wlan_id	A Wireless LAN identifier between 1 and 16.

Defaults

None.

Examples

```
> config wlan security l2tp encryption aes 1
```

Related Commands

show wlan

config wlan security l2tp ike dh-group

To configure IKE used on the wireless LAN, use the **config wlan security l2tp ike dh-group** command.

config wlan security l2tp ike dh-group *wlan_id* **{group-1 | group-2 | group-5}**

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the Wireless LAN security policy.
l2tp	Configure L2tp.
ike dh-group	Configure IKE's Diffie-Hellman Group.
wlan_id	A Wireless LAN identifier between 1 and 16.
{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 l2tp ike dh-group 1 group-2
```

Related Commands

show wlan

config wlan security l2tp ike lifetime

To configures IKE's lifetime parameters used on the wireless LAN, use the **config wlan security l2tp ike lifetime** command.

config wlan security l2tp ike lifetime *wlan_id seconds*

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the Wireless LAN security policy.
l2tp	Configure L2tp.
ike lifetime	Configure IKE's lifetime parameters.
wlan_id	A Wireless LAN identifier between 1 and 16.
seconds	The IKE lifetime in seconds, between 1800 and 345600.

Defaults

None.

Examples

```
> config wlan security l2tp ike lifetime 1 2000
```

Related Commands

show wlan

config wlan security l2tp ike phase1

To configure IKE's phase one mode used on the wireless LAN, use the **config wlan security l2tp ike phase1** command.

config wlan security l2tp ike phase1 main *wlan_id*

Syntax Description

config	Configure parameters.
wlan	Wireless LAN parameters.
security	Configure the Wireless LAN security policy.
l2tp	L2tp.
ike phase1	Configure IKE's phase one mode.
main	Enable the IKE main mode.
wlan_id	A Wireless LAN identifier between 1 and 16.

Defaults

None.

Examples

```
> config wlan security l2tp ike phase1 main 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.
wlan_id	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.
wlan_id	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 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 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.
wlan_id	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.
key	Enter WEP key in ascii
key-index	Key index (1 to 4).

Defaults

None.

Examples

```
> config wlan security wpa 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.
{*wlan_id* | **foreignAp}**	• Enter a Wireless LAN identifier between 1 and 16. • Enter **foreignAp** for third party access points.
{*acl_name* **| 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.
{*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 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.
wlan_id	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.
wlan_id	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 | disable} *wlan_id key*

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.
wlan_id	Wireless LAN identifier between 1 and 16.
key	WPA pre-shared key. Required only if you enable WPA-PSK.

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
wlan_id	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
wlan_id	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 | disable} *wlan_id key*

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.
wlan_id	Wireless LAN identifier between 1 and 16.
[*key***]**	WPA pre-shared key. Required only if you enable WPA2-PSK.

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.
wlan_id	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.
wlan_id	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.
{*wlan_id* | **foreignAp}**	• Enter a Wireless LAN identifier between 1 and 16. • Enter **foreignAp** for third party access points.
seconds	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

Saving Configurations

Use the save config command before you log out of the command line interface to save all previous configuration changes.

- *save config*

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 ap-config

To restore a Cisco 1000 Series lightweight access point configuration database to its factory default, use the **clear ap-config** command.

clear ap-config *Cisco_AP*

Syntax Description

clear	Clear selected configuration elements.
ap-config	Reset Cisco 1000 Series lightweight access point configuration data to factory defaults.
Cisco_AP	Name of the Cisco 1000 Series lightweight access point.

Defaults

None.

Examples

```
> clear ap-config aire1
```

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 arp

To clear the ARP table to a Cisco 1000 Series lightweight access point its factory default, use the **clear arp** command.

clear arp

Syntax Description

clear	Clear selected configuration elements.
arp	Clear the ARP table.

Defaults

None.

Examples

```
> clear arp

Are you sure you want to clear the ARP cache? (y/n)
```

Related Commands

clear transfer, **clear download filename**, **clear download mode**, **clear download path**, **clear download serverip**, **clear download start**, **clear upload datatype**, **clear upload filename**, **clear upload mode**, **clear upload path**, **clear upload serverip**, **clear upload start**

clear 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 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

```
> clear stats mobility

Mobility stats cleared.
```

Related Commands

clear transfer, **clear download datatype**, **clear download filename**, **clear download mode**, **clear download serverip**, **clear download start**, **clear upload datatype**, **clear upload filename**, **clear upload mode**, **clear upload path**, **clear upload serverip**, **clear upload start**, **clear stats port**

clear stats port

To clear statistics counters for a specific port, use the **clear stats port** command.

clear stats port *port*

Syntax Description

clear	Clear selected configuration elements.
stats	Clear statistics counters.
port	Clear statistics counters for a specific port.
port	Physical interface port number.

Defaults

None.

Examples

```
> clear stats port 9
```

Related Commands

clear transfer, **clear download datatype**, **clear download filename**, **clear download mode**, **clear download serverip**, **clear download start**, **clear upload datatype**, **clear upload filename**, **clear upload mode**, **clear upload path**, **clear upload serverip**, **clear upload start**

clear stats 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 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 transfer

To clear the transfer information, use the **clear transfer** command.

clear transfer

Syntax Description

clear	Clear selected configuration elements.
transfer	Clear the transfer information.

Defaults

None.

Examples

```
> clear transfer

Are you sure you want to clear the transfer information? (y/n) y

Transfer Information Cleared.
```

Related Commands

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

```
> clear webmessage

Message cleared.
```

Related Commands

clear transfer, **clear download datatype**, **clear download filename**, **clear download mode**, **clear download path**, **clear download serverip**, **clear download start**, **clear upload filename**, **clear upload mode**, **clear upload path**, **clear upload serverip**, **clear upload start**

clear webtitle

To clear the custom web authentication title, use the **clear webtitle** command.

clear webtitle

Syntax Description

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**

clear ext-webauth-url

To clear the external web authentication URL, use the **clear ext-webauth-url** command.

clear ext-webauth-url

Syntax Description

clear	Clear selected configuration elements.
ext-webauth-url	Clear the external web authentication URL.

Defaults

None.

Examples

```
> clear ext-webauth-url

URL cleared.
```

Related Commands

clear transfer, **clear download datatype**, **clear download filename**, **clear download mode**, **clear download path**, **clear download serverip**, **clear download start**, **clear upload filename**, **clear upload mode**, **clear upload path**, **clear upload serverip**, **clear upload start**

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 a certificate's private key password, use the **transfer download certpassword** command.

transfer download certpassword [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.
[password]	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}	• 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.

Defaults

None.

Examples

```
> transfer datatype code
```

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 image**, **transfer download start**

transfer download filename

To download a specific file, use the **transfer download filename** command.

transfer download filename *filename*

Syntax Description

transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
filename	Set the TFTP filename.
filename	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 tftp

Syntax Description

transfer	Transfer a file to or from the switch.
download	Transfer a file to the switch.
mode	Set transfer mode.
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 path

To set a specific 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 TFTP Path.
path	Directory path.

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 serverip

To configure the IP address of the TFTP server from which to download information, use the **transfer download serverip** command.

transfer download serverip *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.
ip_address	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................................ Code
TFTP Server IP........................... 172.16.16.78
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ c:\find\off/
TFTP Filename............................ wps_2_0_75_0.aes

This may take some time.
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 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.
timeout	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.
retries	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 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.
key	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 | radio-core-dump | signature | systemtrace | traplog}

Syntax Description

transfer	Transfer a file to or from the switch.
upload	Transfer a file from the switch.
datatype	Set upload file type.
{config | crashfile | errorlog | radio-core-dump | signature | systemtrace | traplog}	• Enter **config** to upload the system's configuration file. • Enter **crashfile** to upload the system's crash file. • Enter **errorlog** to upload the system's error log. • Enter **radio-core-dump** to upload the system's error log. • Enter **signature** to upload the system's signature files. • Enter **systemtrace** to upload the system's trace file. • Enter **traplog** to upload the system's trap log.

Defaults: None.

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 download start**, **transfer upload filename**, **transfer upload mode**, **transfer upload path**, **transfer upload serverip**, **transfer upload 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 TFTP filename.
filename	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 download start**, **transfer upload datatype**, **transfer upload mode**, **transfer upload path**, **transfer upload serverip**, **transfer upload start**

transfer upload mode

To configure the transfer mode, use the **transfer upload mode** command.

transfer upload mode tftp

Syntax Description

transfer	Transfer a file to or from the switch.
upload	Transfer a file from the switch.
mode	Set transfer mode.
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 download start**, **transfer upload datatype**, **transfer upload filename**, **transfer upload path**, **transfer upload serverip**, **transfer upload start**

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 Path.
path	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 download start**, **transfer upload datatype**, **transfer upload filename**, **transfer upload mode**, **transfer upload serverip**, **transfer upload start**

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.
ip_address	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 download start**, **transfer upload datatype**, **transfer upload filename**, **transfer upload mode**, **transfer upload path**, **transfer upload 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 download start**, **transfer upload datatype**, **transfer upload filename**, **transfer upload mode**, **transfer upload path**, **transfer upload serverip**

Troubleshooting

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.

debug lwapp client config

TBD

debug lwapp client error

TBD

debug lwapp client event

TBD

debug lwapp client event detail

TBD

debug lwapp client fwd

TBD

debug lwapp client mgmt

TBD

debug lwapp client packet

TBD

debug lwapp client packet detail

TBD

debug lwapp ids rogue containment

TBD

debug lwapp ids sig

TBD

debug lwapp rm measurement

TBD

debug lwapp rm rouge detection

TBD

debug lwapp rm rouge detector

TBD

test lwapp controller ip

TBD

test lwapp controller name

TBD

test lwapp rm

TBD

show lwapp client config

TBD

show lwapp client rcb

TBD

show lwapp client traffic

TBD

show lwapp ids rogue containment

TBD

show lwapp ids sig

TBD

show lwapp rm neighbor-list

TBD

show lwapp rm rogue ad-hoc

TBD

show lwapp rm rogue ap

TBD

show lwapp rm rogue detector

TBD

show lwapp rm rx-stats

TBD