Cisco SWAN CLI Reference

System Release 2.2

The Cisco SWAN Command Line Interface (CLI) allows operators to connect an ASCII console to a 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. The Using the Cisco SWAN CLI section in the Product Guide describes most of the high-level CLI tasks, and the following sections provide additional information:

- *? command*
- *Help Command*
- *Viewing Configurations*
- *Setting Configurations*
- *Saving Configurations*
- *Clearing Configurations, Logfiles, and Other Functions*
- *Uploading and Downloading Files and Configurations*
- *Troubleshooting*

? 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 the (command name) and the ? (question mark).

Example 1

>**?** (at root level)

Clear	Reset the switch or reset configuration to factory defaults.
Config	Configure switch options and settings.
Debug	Manages system debug options.
Help	Help.
Linktest <MAC addr>	Perform a link test to a specified MAC address.
Logout	Exit this session. Any unsaved changes are lost.
Ping <ip address>	Send ICMP echo packets to a specified IP address.
Reset	Reset options.
Save	Save current switch settings to Non-volatile RAM.
Show	Display switch options and settings.
Transfer	Transfer a file to or from the switch.

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

Example 2

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

shows you that datatype is the only entry at the transfer download level.

Example 3

```
>transfer download datatype ?
<config/code> Enter datatype: config or code.
```

shows you the permissible entries for the transfer download datatype command.

Help Command

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

```
>help
```

Example

```
>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*
- *show 802.11b*
- *show aepi*
- *show acl*
- *show advanced 802.11a*
- *show advanced 802.11b*
- *show advanced client-handoff*
- *show ap*
- *show arp switch*
- *show exclusionlist*
- *show boot*
- *show certificate*
- *show client*
- *show country*
- *show cpu*
- *show custom-web*
- *show debug*
- *show dhcp*
- *show dhcp summary*
- *show eventlog*
- *show ike*
- *show ipsec*
- *show interface*
- *show inventory*
- *show l2tp*
- *show load-balancing*
- *show loginsession*
- *show known*
- *show macfilter*
- *show mgmtuser*
- *show mirror*
- *show mobility statistics*
- *show mobility summary*
- *show msglog*

- *show netuser*
- *show network*
- *show port*
- *show qos queue length all*
- *show radius*
- *show rogue ap*
- *show rogue ap detailed*
- *show rogue ap summary*
- *show rogue adhoc*
- *show rogue client*
- *show route summary*
- *show rules*
- *show run-config*
- *show serial*
- *show sessions*
- *show snmpcommunity*
- *show snmptrap*
- *show snmpv3user*
- *show snmpversion*
- *show spanningtree port*
- *show spanningtree switch*
- *show stats*
- *show switchconfig*
- *show sysinfo*
- *show syslog*
- *show tech-support*
- *show tech-support*
- *show time*
- *show trapflags*
- *show traplog*
- *show watchlist*
- *show wlan*
- *show wlan summary*
- *show wps summary*

show 802.11a

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

```
>show 802.11a
```

Syntax

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
Fast-Roaming 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

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

Defaults (none)

Examples

```
>show 802.11b
```

```
802.11b Network.............................. Enabled
11gSupport................................... Disabled
802.11b Operational Rates
    802.11b 1M Rate.......................... Mandatory
    802.11b 2M Rate.......................... Mandatory
    802.11b 5.5M Rate........................ Mandatory
    802.11b 11M Rate......................... Mandatory
    802.11b 11M Rate......................... Mandatory
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
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
Fast-Roaming 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 aepi

To display external policy server information, use the show aepi command.

>show aepi [summary/detailed]

Syntax		
	show aepi	Command action.
	summary	Display a summary of External Policy Server information.
	detailed	Display detailed External Policy Server information.

Defaults (none)

Examples

```
>show aepi summary
AEPI ACL Name
Index Server Address Port Stats
----- -------------- ---- ---------
```

Related Commands config aepi acl

show acl

To display system Access Control Lists, use the show acl command.

>show acl [summary/detailed]

Syntax	show acl	Command action.
	summary	Display a summary of the Access Control Lists.
	detailed	Display detailed Access Control List information.

Defaults (none)

Examples

```
>acl summary
ACL Name                         Applied
-------------------------------- -------
Pubs Only                        Yes
Macnica                          Yes
```

Related Commands config interface acl

SHOW ADVANCED 802.11A COMMANDS

Use the following show advanced 802.11a commands:

- *show advanced 802.11a channel*
- *show advanced 802.11a group*
- *show advanced 802.11a logging*
- *show advanced 802.11a monitor*
- *show advanced 802.11a txpower*
- *show advanced 802.11a profile*
- *show advanced 802.11a summary*

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	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................................... unknown
    Average................................... unknown
    Maximum................................... unknown
  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

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

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	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 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 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	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.
  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 AP performance profiles, use the show advanced 802.11a profile command.

>**show advanced 802.11a profile global**

>**show advanced 802.11a profile <AP name>**

Syntax	show	Display configurations.
	advanced	Advanced parameters.
	802.11a	802.11a network.
	profile	Cisco Radio performance profile.

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 AP 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 AP name, channel, and transmit level summary, use the show advanced 802.11a summary command.

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

Syntax	show	Display configurations.
	advanced	Advanced parameters.
	802.11a	802.11a network.
	summary	AP 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
```

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 following show advanced 802.11b commands:

- *show advanced 802.11b channel*
- *show advanced 802.11b group*
- *show advanced 802.11b logging*
- *show advanced 802.11b monitor*
- *show advanced 802.11b receiver*
- *show advanced 802.11b txpower*
- *show advanced 802.11b profile*
- *show advanced 802.11b summary*

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	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	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	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
   TxPower 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	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		
	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**

> **show advanced 802.11b profile <AP name>**

Syntax		
	show	Display configurations.
	advanced	Advanced parameters.
	802.11b	802.11b/g network.
	profile	AP performance profile.

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 AP 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

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

show	Display configurations.

	advanced	Advanced parameters.
	802.11b	802.11b/g network.
	summary	AP 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
```

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	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	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 AP entry timers, use the show advanced timers command.

>show advanced timers

Syntax	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:

- *show ap auto-rf*
- *show ap config*
- *show ap stats*
- *show ap summary*
- *show ap wlan*

show ap auto-rf

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

>show ap auto-rf <802.11a/802.11b> <AP name>

Syntax	show	Display configurations.
	ap auto-rf	Cisco Radio.
	<802.11a/802.11b>	802.11a or 802.11b setting.
	<AP name>	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> <AP name>
```

Syntax

show	Display configurations.
ap	Cisco Radio.
<802.11a/802.11b/ general>	802.11a, 802.11b/g or general settings.
<AP name>	Cisco 1000 Series lightweight access point name.

Defaults

(none)

Examples

```
>show ap config 802.11a AP01
Cisco 1000 Series lightweight access point Identi-
fier..... 5
Cisco 1000 Series lightweight access point
Name..... AP01
AP Type..... Cisco
Switch Port Number..... 19
MAC Address..... 00:0b:85:01:05:00
IP Address..... Disabled
Cisco 1000 Series lightweight access point Loca-
tion..... default location
Primary Cisco SWAN Switch..... Pubs
Secondary Cisco SWAN Switch.....
Tertiary Cisco SWAN Switch.....
Administrative State..... ADMIN_ENABLED
Operation State..... REGISTERED
Mirroring Mode..... Disabled
AP Mode..... Local
AP Type..... 5212
Remote AP Debug..... Disabled
S/W  Version..... 2.0.133.0
Boot  Version..... 0.0.0.0
Stats Reporting Period..... 180
Number Of Slots..... 2
Rad Model.....
Rad Serial Number.....

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:85:01:05:00
      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
      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
      Maximum Tx Power Level................ 17

    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...................... 32
      Tx Power Level 2...................... 16
      Tx Power Level 3...................... 8
      Tx Power Level 4...................... 4
      Tx Power Level 5...................... 1
      Tx Power Level 6...................... 0
      Tx Power Level 7...................... 0
      Tx Power Level 8...................... 0
      Tx Power Configuration................ CUSTOMIZED
      Current Tx Power Level................ 5

    Phy OFDM parameters
      Configuration......................... CUSTOMIZED
      Current Channel....................... 64
      TI Threshold.......................... -50
      Antenna Type.......................... EXTERNAL_ANTENNA
      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..................... 00
```

>show ap config 802.11b AP01

```
Cisco 1000 Series lightweight access point Identi-
fier..................... 5
```

```
Cisco 1000 Series lightweight access point
Name.............................. AP01
AP Type.......................................... Cisco SWAN
Switch Port Number............................... 19
MAC Address...................................... 00:0b:85:01:05:00
IP Address....................................... Disabled
Cisco 1000 Series lightweight access point Loca-
tion............................ default location
Primary Cisco SWAN Switch.........................
Secondary Cisco SWAN Switch.......................
Tertiary Cisco SWAN Switch........................
Administrative State............................. ADMIN_ENABLED
Operation State.................................. REGISTERED
Mirroring Mode................................... Disabled
AP Mode.......................................... Local
Remote AP Debug.................................. Disabled
S/W  Version..................................... 2.0.133.0
Boot  Version.................................... 0.0.0.0
Stats Reporting Period........................... 180
Number Of Slots.................................. 2
Rad Model.....................................
Rad Serial Number.............................

Attributes for Slot  1
    Radio Type................................... RADIO_TYPE_80211b
    Administrative State......................... ADMIN_ENABLED
    Operation State.............................. DOWN
    WLAN Override................................ Disabled
    CellId....................................... 0

    Station Configuration
      Configuration.............................. AUTOMATIC
      Number Of WLANs............................ 0
      Medium Occupancy Limit..................... 100
      CFP Period................................. 4
      CFP MaxDuration............................ 60
      BSSID...................................... 00:0b:85:01:05:00
      Operation Rate Set
        1000 Kilo Bits........................... MANDATORY
        2000 Kilo Bits........................... MANDATORY
        5500 Kilo Bits........................... MANDATORY
        11000 Kilo Bits.......................... MANDATORY
      Beacon Period.............................. 100
      DTIM Period................................ 1
      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
      Maximum Tx Power Level..................... 30

    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........................... 32
      Tx Power Level 2........................... 16
      Tx Power Level 3........................... 8
      Tx Power Level 4........................... 4
      Tx Power Level 5........................... 1
      Tx Power Level 6........................... 0
      Tx Power Level 7........................... 0
      Tx Power Level 8........................... 0
      Tx Power Configuration..................... AUTOMATIC
      Current Tx Power Level..................... 1

    Phy DSSS parameters
      Configuration.............................. AUTOMATIC
      Current Channel............................ 1
      Current CCA Mode........................... 0
      ED Threshold............................... -50
      Antenna Type............................... EXTERNAL_ANTENNA
      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 AP1
Cisco 1000 Series lightweight access point Identi-
fier.......................... 5
Cisco 1000 Series lightweight access point
Name.............................. AP01
AP Type.......................................... Cisco SWAN
Switch Port Number............................... 19
MAC Address...................................... 00:0b:85:01:05:00
IP Address....................................... Disabled
Cisco 1000 Series lightweight access point Loca-
tion........................... default location
Primary Switch.................................
Administrative State............................. ADMIN_ENABLED
Operation State.................................. REGISTERED
Mirroring Mode................................... Disabled
AP Mode.......................................... Local
Remote AP Debug.................................. Disabled
S/W  Version..................................... 2.0.133.0
Boot  Version.................................... 0.0.0.0
Stats Reporting Period........................... 180
Number Of Slots.................................. 2
Rad Model.....................................
Rad Serial Number................................ 01012203-10057105-01182
```

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

show ap stats

To display the statistics for an 802.11b/g Cisco 1000 Series lightweight access point, use the show ap stats command.

```
>show ap stats <802.11a/802.11b> <AP name>
```

Syntax

show	Display configurations.
ap	Cisco Radio.
<802.11a/802.11b>	802.11a or 802.11b/g statistics.
<AP name>	Cisco 1000 Series lightweight access point name.

Defaults (none)

Examples

```
>show ap stats 802.11b AP01
Number Of Slots.................................. 2
Rad Name......................................... AP01
MAC Address...................................... 00:0b:85:01:05:00
  Radio Type..................................... RADIO_TYPE_80211a
  Stats Information
    Number of Users.............................. 0
    TxFragmentCount.............................. 24904
    MulticastTxFrameCnt.......................... 11710
    FailedCount.................................. 91534
    RetryCount................................... 5582
    MultipleRetryCount........................... 0
    FrameDuplicateCount.......................... 0
    RtsSuccessCount.............................. 0
    RtsFailureCount.............................. 0
    AckFailureCount.............................. 473136
    RxFragmentCount.............................. 12978548
    MulticastRxFrameCnt.......................... 0
    FcsErrorCount................................ 230771
    TxFrameCount................................. 24904
    WepUndecryptableCount........................ 130
```

Related Commands config ap stats-timer

show ap summary

To display a summary of all APs attached to the Cisco Wireless LAN Controller, use the show ap summary command. A list containing each AP name, number of slots, manufacturer, MAC address, location and Cisco Wireless LAN Controller port number will be displayed.

```
>show ap summary
```

Syntax

show	Display configurations.
ap	All APs.
summary	Summary of all APs.

Defaults (none)

Examples

```
>show ap summary
AP Name            Slots AP Type   MAC Addr          Location         Port
------------------ ----- --------- ----------------- ---------------- ----
AP03               2     Cisco SWAN 00:0b:85:01:18:b0 default location 12
AP02               2     Cisco SWAN 00:0b:85:01:12:60 default location 11
AP01               2     Cisco SWAN 00:0b:85:01:05:00 default location 19
```

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 WLAN Override mode (as described in the Product Guide), use the show ap wlan command.

```
>show ap wlan [802.11a/802.11b] <AP Name>
```

Syntax	show	Display configurations.
	ap	All APs.
	wlan	WLAN parameter.
	<802.11a/802.11b>	802.11a or 802.11b/g statistics.
	<AP name>	Cisco 1000 Series lightweight access point name.

Defaults (none)

Examples

```
>show ap wlan 802.11a AP01
Cisco 1000 Series lightweight access point 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	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 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.

Note: Use the **show exclusionlist** command to view clients on the Exclusion List.

```
>show exclusionlist
```

Syntax	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	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 following show certificate commands:

- *show certificate compatibility*
- *show certificate summary*

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	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	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 following show client commands:

- *show client ap*
- *show client detail*
- *show client summary*
- *show client username*

show client ap

To display the clients on an 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 blacklist** command to view clients on the Exclusion List (blacklisted).

```
>show client ap <802.11a/802.11b> <AP name>
```

Syntax	show	Display configurations.
	ap	Cisco Radio.
	<802.11a/802.11b>	802.11a or 802.11b/g clients.
	<AP name>	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 blacklist

show client detail

To display detailed information for a client on an 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 blacklist** command to view clients on the Exclusion List (blacklisted).

```
>show client detail <MAC address>
```

Syntax

show	Display configurations.
client	802.11a or 802.11b/g client.
detail	Connectivity information.
<MAC address>	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 blacklist

show client summary

To display a summary of clients associated with an 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 blacklist** command to view clients on the Exclusion List (blacklisted).

```
>show client summary
```

Syntax

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

Defaults (none)

Examples

```
>show client summary
MAC Address       AP Name           Status        WLAN Auth Protocol Port
----------------- ----------------- ------------- ---- ---- -------- ----
00:0c:41:0a:33:13 AP01              Associated    1    No   802.11g  5
```

Related Commands show client ap, show client detail, show client username, show blacklist

show client username

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

```
>show client username <Username>
```

Syntax

show	Display configurations.
username	Cisco Radio.
<Username>	Client 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.

```
>show country
```

Syntax

show	Display configuration options.
country	Supported Countries.

Defaults (none)

Examples

```
>show country
Supported Country Codes
   AT..................................... 802.11a/802.11b/802.11g
   AU..................................... 802.11a/802.11b/802.11g
   BE..................................... 802.11a/802.11b/802.11g
   CA..................................... 802.11a/802.11b/802.11g
   DE..................................... 802.11a/802.11b/802.11g
   DK..................................... 802.11a/802.11b/802.11g
   EE..................................... 802.11a/802.11b/802.11g
   ES..................................... 802.11b/802.11g
   FI..................................... 802.11a/802.11b/802.11g
   FR..................................... 802.11a/802.11b/802.11g
   GB..................................... 802.11a/802.11b/802.11g
   GR..................................... 802.11b/802.11g
   HK..................................... 802.11a/802.11b/802.11g
   HU..................................... 802.11a/802.11b/802.11g
   IE..................................... 802.11a/802.11b/802.11g
   IN..................................... 802.11b/802.11g
   IS..................................... 802.11a/802.11b/802.11g
   IT..................................... 802.11a/802.11b/802.11g
   JP..................................... 802.11a/802.11b/802.11g
   KR..................................... 802.11a/802.11b
   NZ..................................... 802.11a/802.11b/802.11g
   NO..................................... 802.11a/802.11b/802.11g
   PL..................................... 802.11a/802.11b/802.11g
   PT..................................... 802.11a/802.11b/802.11g
   SE..................................... 802.11a/802.11b/802.11g
   SG..................................... 802.11a/802.11b/802.11g
   SI..................................... 802.11a/802.11b/802.11g
   SK..................................... 802.11a/802.11b/802.11g
   TH..................................... 802.11b/802.11g
   TW..................................... 802.11a/802.11b/802.11g
   US..................................... 802.11a/802.11b/802.11g
   USL.................................... 802.11a/802.11b/802.11g
   USE.................................... 802.11a/802.11b/802.11g
   ZA..................................... 802.11a/802.11b/802.11g

Configured Country..................... United States (Legacy)
```

Note: The Cisco Wireless LAN Controller Country Code only operates with Cisco 1000 Series lightweight access points designed for operation in the associated Regulatory Domain. Refer to the Cisco SWAN Supported Country Codes in the Product Guide for Cisco Wireless LAN Controller Country Code mapping to Cisco 1000 Series light-weight access point Regulatory Domains.

Related Commands show sysinfo

show cpu

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

```
>show cpu
```

Syntax 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	show custom-web	Command action.

Defaults (none)

Examples

```
>show custom-web
Cisco SWAN Logo................................ Enabled
CustomLogo..................................... Disabled
Custom Title................................... Disabled
Custom Message................................. Disabled
Custom Redirect URL............................ Disabled
External Web Authentication Mode............... Disabled
External Web Authentication URL................ Disabled
```

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	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 DHCP server configuration.

>show dhcp <scope name>

Syntax	show dhcp	Command action.
	<scope name>	The scope name set with the config dhcp command.

Defaults None

Examples

```
>show dhcp 003
Enabled.................................... No
```

```
Lease Time..................................... 0
Pool Start..................................... 0.0.0.0
Pool End....................................... 0.0.0.0
Network........................................ 0.0.0.0
Netmask........................................ 0.0.0.0
Default Routers................................ 0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain.....................................
DNS............................................ 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers........................... 0.0.0.0 0.0.0.0 0.0.0.0
```

Related Commands config dhcp, show dhcp summary

show dhcp summary

Use the show dhcp summary command, to display a summary of DHCP server configurations.

>show dhcp summary

Syntax	show dhcp	Command action.
	summary	List information about DHCP servers.

Defaults None

Examples

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

Related Commands config dhcp, show dhcp

show eventlog

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

>show eventlog

Syntax	show	Display configurations.
	eventlog	System events.

Defaults (none)

Examples

```
>show eventlog
       File     Line TaskID   Code        d  h  m  s
EVENT> nim.c     154 1234B2DC 00000000    0  0  0 44
EVENT> bootos.c  447 12346F44 AAAAAAAA    0  0  0 17
EVENT> nim.c     154 121160B4 00000000    0  0  0 44
EVENT> bootos.c  447 12111D1C AAAAAAAA    0  0  0 17
EVENT> nim.c     154 121180A4 00000000    0  0  0 44
EVENT> bootos.c  447 12113C24 AAAAAAAA    0  0  0 17
EVENT> nim.c     154 1210D5CC 00000000    0  0  0 44
EVENT> bootos.c  445 12109154 AAAAAAAA    0  0  0 17
EVENT> nim.c     154 121176C4 00000000    0  0  0 44
EVENT> bootos.c  445 12113244 AAAAAAAA    0  0  0 17
EVENT> nim.c     154 121176C4 00000000    0  0  0 43
EVENT> bootos.c  445 12113244 AAAAAAAA    0  0  0 17
EVENT> nim.c     154 121176C4 00000000    0  0  0 44
EVENT> bootos.c  445 12113244 AAAAAAAA    0  0  0 17
EVENT> nim.c     154 1210D44C 00000000    0  0  0 42
Would you like to display the next 15 entries? (y/n)
```

Related Commands show msglog

show ike

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

>show ike

Syntax	show	Command action.
	ike	Display 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

Syntax	show	Command action.
	ipsec	Display active IPSEC SAs
	<IP or MAC address>	Display active IPSEC SAs.
Defaults	(none)	
Examples	**>show ipsec**	
Related Commands	None	

show interface

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

>show interface [summary/detailed <interface name>]

Syntax	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
-------------------------------  --------  --------------  -------

management                       2         192.168.2.36    Static
service-port                     N/A       172.16.16.199   Static
virtual                          N/A       0.0.0.0         Static
vlan_301                         301       192.168.2.200   Dynamic
```

>show interface detailed management

```
Interface Name................................ management
MAC Address................................... 00:0b:85:02:0d:20
IP Address.................................... 192.168.2.36
IP Netmask.................................... 255.255.255.0
IP Gateway.................................... 192.168.2.1
```

```
VLAN..................................... 2
Physical Port............................ 1
Primary DHCP Server...................... 10.1.2.11
Secondary DHCP Server.................... Unconfigured
ACL...................................... Unconfigured
```

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	show	Display configurations.
	inventory	Physical Cisco Wireless LAN Controller configuration.

Defaults (none)

Examples

```
>show inventory
Switch Description....................... Controller
Machine Model............................ AIR-WLC4136-K9
Serial Number............................ 102389954
Burned-in MAC Address.................... 00:0B:85:02:01:00
Gig Ethernet/Fiber Card.................. Present
Crypto Accelerator....................... Present
```

Related Commands show sysinfo

show l2tp

To display L2TP sessions, use the show l2tp command.

```
>show l2tp
```

Syntax	show	Display configurations.
	summary	Displays all L2TP sessions.
	<LAC IP addr>	Displays a L2TP session.

Defaults (none)

Examples

```
>show l2tp summary
LAC_IPaddr LTid LSid RTid RSid ATid ASid State
---------- ---- ---- ---- ---- ---- ---- -----
```

Related Commands None

show known

To display known AP information, use the show known command.

```
>show known ap <summary/detailed>
```

Syntax	show	Display configurations.
	known ap	Known AP information.
	<summary/	Displays a list of all Known APs
	detailed>	Provides detailed information for a Known AP

DefaultsExamples

```
>show known ap summary
MAC Address        State       # APs  # Clients   Last Heard
```

```
-----------         -----------  -----   --------   -----------------
```

Related Commands config ap

show load-balancing

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

```
>show load-balancing
```

Syntax	show	Display configurations.
	load-balancing	Status load-balancing.
Defaults	Enabled	

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	show	Display configurations.
	loginsession	Current session details.
Defaults	(none)	

Examples

```
>show loginsession
ID User Name        Connection From  Idle Time     Session Time
-- ---------------  ---------------  ------------  ------------
00 admin            172.18.4.84      00:00:00      01:08:18
```

Related Commands config loginsession close

show macfilter

To display the MAC filter parameters, use the show macfilter commands. 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 WLAN.

```
>show macfilter [summary/detail <MAC address>]
```

Syntax	show	Display configurations.
	macfilter	Filter details.
Defaults	(none)	

Examples

```
>show macfilter summary
MAC Filter RADIUS Compatibility mode.............. Cisco ACS
MAC Filter Delimiter.............................. None

>show macfilter detail
Unable to retrieve MAC filter.
```

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

show		Display configurations.
mgmtuser		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 MIRROR COMMANDS

Use the following show mirror commands.

- *show mirror ap*
- *show mirror foreignap*
- *show mirror mac*
- *show mirror port*

show mirror ap

To view the Cisco 1000 Series lightweight access points whose transmit and receive data appears on the Mirror Port (see *config mirror port*) for troubleshooting, use the show mirror ap command.

```
>show mirror ap
```

Syntax

show		Configure parameters.
mirror		Mirror command.
ap		Cisco 1000 Series lightweight access point.

Defaults (none)

Examples

```
>show mirror ap
AP
-----------------
AP3
```

Related Commands config mirror ap, show mirror foreignap, show mirror mac, show mirror port

show mirror foreignap

To view the Third-Party APs whose transmit and receive data appears on the Mirror Port (see *config mirror port*) for troubleshooting, use the show mirror foreignap command.

```
>show mirror foreignap
```

Syntax	show	Configure parameters.
	mirror	Mirror command.
	foreignap	Third-Party Access Point.

Defaults (none)

Examples

```
>show mirror foreignap
Foreign AP Port
---------------
          2
```

Related Commands config mirror foreignap, show mirror ap, show mirror mac, show mirror port

show mirror mac

To view the clients whose transmit and receive data appears on the Mirror Port (see *config mirror port*) by MAC address, use the show mirror mac command.

```
>show mirror mac
```

Syntax	show	Configure parameters.
	mirror	Mirror command.
	mac	Client MAC address.

Defaults (none)

Examples

```
>show mirror mac
Client MAC        Type
----------------- -------
23:0c:41:0a:33:a3 Static
```

Related Commands config mirror mac, show mirror ap, show mirror foreignap, show mirror port

show mirror port

(Obsolete command.)

SHOW MOBILITY COMMANDS

Use the following show mobility commands.

- *show mobility statistics*
- *show mobility summary*

show mobility statistics

To display the statistics information for the Controller Mobility Groups, use the show mobility statistics command.

```
>show mobility statistics
```

Syntax	show	Display configurations.
	mobility	Controller Mobility Group.
	statistics	Statistics details.

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 summary

To display summary information for the Controller Mobility Groups, use the show mobility summary command.

>show mobility summary

Syntax		
	show	Display configurations.
	mobility	Controller Mobility Group.
	summary	Summary details

Defaults (none)

Examples

```
>show mobility summary
Mobility Protocol Port........................ 16666
Mobility Security Mode........................ Disabled
Mobility Group................................ Eng_Test
Mobility Group members configured............. 1
Switches configured in the Mobility Group
 MAC Address       IP Address                Group Name
 00:0b:85:02:0d:26 10.1.77.170               <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

show	Display configurations.
msglog	Message logs.

Defaults (none)

Examples

```
>show msglog
Fri Aug  8 17:25:51 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:50 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:50 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:49 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:49 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:49 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:35 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:35 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:34 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:34 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:34 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:33 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:22 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:22 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug  8 17:25:21 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
```

Related Commands show eventlog

show netuser

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

>show netuser

Syntax

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

show	Display configurations.
network	Network configuration.

Defaults (none)

Examples

```
>show network
RF/Mobility Domain Name..................... Engr_Test
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Shell (ssh).......................... Enable
Telnet...................................... Disable
Ethernet Multicast Mode..................... Enable
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco 1000 Series lightweight access point Default Master.................
Disable
Mgmt Via Wireless Interface................. Disable
Over The Air Provisioning of APs............ Enable
Mobile Peer to Peer Blocking................ Enable
Apple Talk.................................. Disable
AP Fallback................................. Enable
Web Auth Redirect Ports..................... 80
```

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 number>

>show port summary

Syntax

show	Display configurations.
port	Cisco Wireless LAN Controller port.
<port number>/summary	Individual port or all ports

Defaults (none)

Examples

```
>show port 7
           STP  Admin   Physical Physical   Link   Link    Mcast
Pr Type    Stat Mode    Mode     Status     Status Trap    Appliance POE
-- ------- ---- ------- -------- ---------- ------ ------- -------- ------
7  Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable    Enable

>show port summary
           STP  Admin   Physical Physical   Link   Link    Mcast
Pr Type    Stat Mode    Mode     Status     Status Trap    Appliance POE
-- ------- ---- ------- -------- ---------- ------ ------- --------  ------
1  Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
2  Normal  Disa Disable Auto     10 Half    Down   Enable  Enable   Enable
3  Normal  Disa Disable Auto     10 Half    Down   Enable  Disable  Enable
4  Normal  Disa Disable Auto     10 Half    Down   Enable  Disable  Enable
5  Normal  Disa Disable Auto     10 Half    Down   Enable  Disable  Enable
6  Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
7  Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
8  Normal  Disa Disable Auto     10 Half    Down   Enable  Disable  Enable
9  Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
```

```
10 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
11 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
12 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
13 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
14 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
15 Normal  Disa Enable  Auto     10 Half    Down   Enable  Disable  Enable
16 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
17 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
18 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
19 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
20 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
21 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
22 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
23 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
24 Normal  Disa Enable  Auto     10 Half    Down   Enable  Enable   Enable
```

Related Commands config ap port, config network dsport, config mirror port, config port admin-mode, 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	show qos	Command action
	queue_length all	Display all quality of service queue lengths.

Defaults (none)

Examples **>show qos queue_length all**

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

Related Commands config qos

SHOW RADIUS COMMANDS

Use the following show radius commands:

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

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	show	Display configurations.

	radius acct	RADIUS accounting server.
	statistics	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	show	Display configurations.
	radius auth	RADIUS authentication server.
	statistics	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 summary

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

>show radius summary

Syntax	show	Display configurations.
	radius	RADIUS authentication server.
	summary	server summary.

Defaults (none)

Examples

```
>show radius summary

Vendor Id Backward Compatibility..... Enabled
Credentials Caching.................. Enabled
Call Station Id Type................. IP Address

Authentication Servers
Index  Server Address                                 Port   State
-----  --------------------------------------------- ------ --------------
1      10.1.3.10                                     1812   Accounting
Servers
Index  Server Address                                 Port   State
-----  --------------------------------------------- ------ --------------
1      10.1.3.10                                     1813   Enabled
```

Related Commands show radius auth statistics, show radius acct statistics

SHOW ROGUE AP COMMANDS

Use the following Rogue AP commands:

- *show rogue ap clients*
- *show rogue ap detailed*
- *show rogue ap summary*

show rogue ap clients

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

```
>show rogue ap clients <Rogue AP MAC address>
```

Syntax	show	Display configurations.
	rogue ap	Rogue access points.
	clients	Summary information.
	<Rogue AP MAC address>	Rogue AP MAC address.

Defaults (none)

Examples

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

MAC Address        State     # APs   Last Heard
-----------------  ------    1       --------------------------
00:0b:85:01:39:13  Alert     1       Tue Oct 5 11:36:44 2004
```

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 address>

Syntax	show	Display configurations.
	rogue ap	Rogue access points.
	detailed	Summary information.
	<MAC address>	AP MAC address.

Defaults (none)

Examples **>show rogue ap detailed 00:40:96:90:d1:6a**

```
Rogue MAC Address.............................. 00:40:96:90:d1:6a
State.......................................... Alert
First Time Rogue was Reported.................. Sat Aug  9 15:48:50 2003
Last Time 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 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	show	Display configurations.
	rogue ap	Rogue access points.
	summary	Summary information.

Defaults (none)

Examples **>show rogue ap summary**

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

MAC Address        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     Sat 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 ap detailed, show rogue ap clients

SHOW ROGUE ADHOC COMMANDS

Use the following Rogue AP commands:

- *show rogue adhoc detailed*
- *show rogue adhoc summary*

show rogue adhoc detailed

To show details of an adhoc rogue access detected by the Cisco Wireless LAN Controller, use the show rogue adhoc client detailed command.

>show rogue adhoc detailed <Adhoc Rogue MAC address>

Syntax	show	Display configurations.
	rogue adhoc	Adhoc Rogue.
	detailed	Summary information.
	<MAC address>	Adhoc 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 rogues detected by the Cisco Wireless LAN Controller, use the show rogue adhoc summary command.

>show rogue adhoc summary

Syntax	show	Display configurations.
	rogue adhoc	Adhoc Rogue.
	summary	Summary information.

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:

- *show rogue client detailed*

- *show rogue client summary*

show rogue client detailed

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

>show rogue client detailed <MAC address>

Syntax	show	Display configurations.
	rogue client	Rogue client.
	detailed	Summary information.
	<MAC address>	Rogue client MAC address.
Defaults	(none)	

Examples >**show rogue client detailed 00:40:96:90:d1:6a**

```
Rogue Client MAC Address..................... 00:40:96:90:d1:6a
State........................................ Alert
First Time Rogue Client was Reported.......... Sat Aug  9 15:48:50 2003
Last Time Rogue Client was Reported........... Sat Aug  9 21:16:50 2003
Reported By
    AP 1
        Rogue Client 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 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	show	Display configurations.
	rogue client	Rogue client.
	summary	Summary information.
Defaults	(none)	

Examples >**show rogue client summary**

```
MAC Address        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     Sat 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 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	show route	Command action
	summary	Summary information.

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	show rules	Command action

Defaults (none)

Examples **>show rules**

Related Commands None

show run-config

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

>show run-config

Syntax	show run-config	Command action.

Defaults (none)

Examples

```
>show run-config
System Inventory
System Inventory
Switch Description.............................. Cisco 1000 Series light-
weight access point
Machine Model................................... 4112
Serial Number................................... 01012403-10037905-01007
Burned-in MAC Address........................... 00:0B:85:02:0D:20
Gig Ethernet/Fiber Card......................... Present
Crypto Accelerator.............................. Present

System Information
Manufacturer's Name............................. Cisco SWAN
Product Name.................................... Cisco 1000 Series light-
weight access point
```

```
Product Version.................................. 2.0.133.0
RTOS Version..................................... 2.0.133.0
Bootloader Version............................... 2.0.133.0

System Name...................................... Pubs01
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.45.3.60.1
IP Address....................................... 10.1.44.170
System Up Time................................... 1 days 2 hrs 15 mins 28
secs

Configured Country............................... United States (Legacy)
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +46 C

State of 802.11b Network......................... Disabled
State of 802.11a Network......................... Enabled
Number of WLANs.................................. 1
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 1

Switch Configuration
802.3x Flow Control Mode......................... Enable
Current LWAPP Transport Mode..................... Layer 2
LWAPP Transport Mode after next switch reboot.... Layer 2

Network Information
RF/Mobility Domain Name..................... Engr_Test
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Shell (ssh)........................... Enable
Telnet...................................... Disable
Ethernet Multicast Mode..................... Enable
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master................. Disable
Mgmt Via Wireless Interface................. Disable
Over The Air Provisioning of APs............ Enable
Mobile Peer to Peer Blocking................ Enable
Apple Talk.................................. Disable
AP Fallback................................. Enable
Web Auth Redirect Ports..................... Enable

Port Summary
           STP   Admin   Physical   Physical   Link   Link   Mcast
Pr  Type   Stat   Mode     Mode      Status   Status  Trap   Appliance POE
-- ------- ---- ------- ---------- ---------- ------ ------- ------- ------
1  Normal  Forw Enable  Auto       100 Full   Up     Enable  Enable  Enable
2  Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
3  Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
4  Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
5  Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
6  Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
7  Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
8  Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
9  Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
10 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
11 Normal  Forw Enable  Auto       100 Full   Up     Enable  Enable  Enable
12 Normal  Forw Enable  Auto       100 Full   Up     Enable  Enable  Enable
```

```
13 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
14 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
15 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
16 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
17 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
18 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
19 Normal  Forw Enable  Auto       100 Full   Up     Enable  Enable  Enable
20 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
21 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
22 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
23 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
24 Normal  Disa Enable  Auto       10 Half    Down   Enable  Enable  Enable
25 Normal  Forw Enable  1000 Full  1000 Full  Up     Enable  Enable  N/A

AP Summary
AP Name            Slots AP Type   MAC Addr          Location          Port
------------------ ----- --------- ----------------- ----------------  ----
AP03                2    Cisco SWAN 00:0b:85:01:18:b0  default location  12
AP02                2    Cisco SWAN 00:0b:85:01:12:60  default location  11
AP01                2    Cisco SWAN 00:0b:85:01:05:00  default location  19

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	show	Display configurations.
	serial	Console serial port.
Defaults	9600, 8, OFF, 1, (none)	

Examples

```
>show serial
Serial Port Login Timeout (minutes)..... 0
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	show	Display configurations.
	sessions	CLI session limits.
Defaults	5 minutes, 5 sessions.	

Examples

```
>show sessions
CLI Login Timeout (minutes)..... 0
```

```
Maximum Number of CLI Sessions..... 5
```

which 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 a show the SNMP version 1/version 2c community configuration, use the show snmpcommunity command.

>show snmpcommunity

Syntax	show	Display configurations.
	snmpcommunity	SNMP version 1/version 2c community configuration.

Defaults (none)

Examples

```
>show snmpcommunity
SNMP Community Name Client IP Address Client IP Mask   Access Mode Status
------------------- ----------------- ---------------- ----------- ------
**********          0.0.0.0           0.0.0.0          Read/Write  Enable
public              0.0.0.0           0.0.0.0          Read Only   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	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	show	Display configurations.
	snmpv3user	SNMP version 3 configuration.

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		
	show	Display configurations.
	snmpversion	SNMP states.

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.

>show spanningtree port <port>

Syntax		
	show	Display configurations.
	spanningtree	Spanning tree.
	port	Physical port.
	<port>	Physical port number: - 1 through 4 on Cisco 2000 Series Wireless LAN Controller - 1 or 2 on Cisco 4100 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	show	Display configurations.
	spanningtree	Spanning tree.
	switch	Cisco Wireless LAN Controller configuration.
	<port>	Physical port number: - 1 through 4 on Cisco 2000 Series Wireless LAN Controller - 1 or 2 on Cisco 4100 Series Wireless LAN Controller

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 forward-delay, config spanningtree switch hellotime, config spanningtree switch maxage, config spanningtree switch mode

SHOW STATS COMMANDS

Use the following show stats commands:

- *show stats port*
- *show stats switch*

show stats port

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

>show stats port detailed <port>

>show stats port summary <port>

Syntax	show	Display configurations.
	stats	Statistics.
	port	Port.
	detailed	Details for a port.
	summary	Summary of all ports.
	<port>	Physical port number: - 1 through 4 on Cisco 2000 Series Wireless LAN Controller - 1 or 2 on Cisco 4100 Series Wireless LAN Controller

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


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

RECEIVED PACKETS NOT FORWARDED
Total.......................................... 0
Local Traffic Frames:0              RX Pause Frames     :0
Unacceptable Frames :0              VLAN Membership     :0
VLAN Viable Discards:0              MulticastTree Viable:0
ReserveAddr Discards:0
CFI Discards        :0              Upstream Threshold  :0

PACKETS TRANSMITTED (OCTETS)
Total Bytes.................................... 52132995
64 byte pkts        :647066         65-127 byte pkts    :28346
128-255 byte pkts   :26988          256-511 byte pkts   :11595
512-1023 byte pkts  :114            1024-1518 byte pkts :1324
1519-1530 byte pkts :0              Max Info            :1522

PACKETS TRANSMITTED SUCCESSFULLY
Total.......................................... 715435
Unicast Pkts  :117570         Multicast Pkts:597864      Broadcast Pkts:1


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

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

PROTOCOL STATISTICS
BPDUs Received      :1450           BPDUs Transmitted   :0
802.3x RX PauseFrame:0

Time Since Counters Last Cleared............... 6 day 23 hr 49 min 1 sec
```

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

>show stats switch summary

Syntax

show	Display configurations.
stats	Statistics.
switch	Cisco Wireless LAN Controller.
detailed	Details for a port.
summary	Summary of all ports.

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

VLAN ENTRIES
Maximum........................................ 128
Most Ever Used.................................. 1
Static In Use................................... 1
Dynamic In Use.................................. 0
VLANs Deleted................................... 0
Time Since Ctrs Last Cleared.................... 2 day 11 hr 23 min 43 sec
```

Related Commands config network dsport

show switchconfig

To a show the network (DS Port) 802.3x flow control mode, use the show switchconfig command.

>show switchconfig

Syntax

show	Display configurations.
switchconfig	Cisco Wireless LAN Controller configuration.

Defaults (none)

Examples

```
>show switchconfig
802.3x Flow Control Mode..................... Disable
Current LWAPP Transport Mode................. Layer 2
LWAPP Transport Mode after next switch reboot . Layer 2
```

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

show	Display configurations.
sysinfo	Cisco Wireless LAN Controller information.

Defaults (none)

Examples

```
>show sysinfo
Manufacturer's Name.......................... <company name>
Product Name................................. Controller
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

show	Display configurations.

	syslog	Cisco Wireless LAN Controller SNMP trap logging status or target IP Address.

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	show	Display configurations.
	tech-support	Cisco Wireless LAN Controller variables.

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	show	Display configurations.
	time	Cisco Wireless LAN Controller time and date.

Defaults (none)

Examples

```
>show time
Time..................................... Sun Aug 10 03:04:51 2004

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

show		Display configurations.
trapflags		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 SWAN 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

show		Display configurations.
traplog		Cisco Wireless LAN Controller SNMP trap log.

Defaults (none)

Examples

```
>show traplog
Number of Traps Since Last Reset ............ 1316
Number of Traps Since Log Last Displayed .... 6

Log System Time              Trap
--- ------------------------ ----------------------------------------
  0 Sun Aug 10 03:13:03 2003 Rogue AP: 00:0b:85:01:2f:90 removed from AP:0
                             0:0b:85:01:18:b0 Interface no:1(unknowntype)
 1 Sun Aug 10 03:10:06 2003 Rogue AP: 00:0b:85:01:02:40 removed from AP:0
                             0:0b:85:01:18:b0 Interface no:1(unknowntype)
  2 Sun Aug 10 03:10:06 2003 Rogue AP: 00:0b:85:01:4c:90 removed from AP:0
                             0:0b:85:01:18:b0 Interface no:1(unknowntype)
  3 Sun Aug 10 03:07:53 2003 Rogue AP: 00:0b:85:01:2e:30 detected on AP:00
                             :0b:85:01:18:b0  Interface no:1(unknown
                             type) with RSSI: -66 and SNR: 29
  4 Sun Aug 10 03:05:53 2003 Rogue AP: 00:40:96:40:82:89 detected on AP:
                             00:0b:85:01:18:b0  Interface no:1(unknown
                             type) with RSSI: -68 and SNR: 27
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

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/disable, config watchlist add

show wlan

To show a summary of the Cisco Wireless LAN Controller WLANs and their status, use the show wlan summary command.

>show wlan <WLAN id> foreignAp

Syntax		
	show	Display configurations.
	wlan	Wireless LAN.
	summary	Displays a summary of all WLANs.
	<WLAN id>	Cisco SWAN WLAN 1 through 17 (17 = foreignAp).
	foreignAp	Cisco SWAN WLAN 17.

Defaults (none)

Examples

```
>show wlan 1
WLAN Identifier.............................. 1
Network Name (SSID).......................... Controller
Status....................................... Enabled
MAC Filtering................................ Disabled
AAA Policy Override.......................... Disabled
External Policy Server....................... Disabled
Number of Active Clients..................... 1
Exclusionlist................................ Disabled
Session Timeout.............................. Infinity
Interface.................................... management
DHCP Server.................................. 10.1.2.119
Quality of Service........................... Bronze (low)
WME.......................................... Allowed
Wired Protocol............................... None
Radio Policy................................. All
Security
   802.11 Authentication:.................... Open System (Allow shared key)
   Static WEP Keys........................... Enabled
        Key Index:.............................. 1
        Encryption:............................. 104-bit WEP
   802.1X.................................... Disabled
   Wi-Fi Protected Access.................... Disabled
   Robust Secure Network..................... Disabled
   IP Security............................... Disabled
   IP Security Passthru...................... Disabled
   L2TP...................................... Disabled
   Web Based Authentication.................. Disabled
   Cranite Passthru.......................... Disabled
   Fortress Passthru......................... Disabled

>show wlan 17 (or show wlan foreignAp)
WLAN Identifier.............................. 17
Network Name (SSID).......................... Lobby
Status....................................... Enabled
MAC Filtering................................ Disabled
```

```
AAA Policy Override..................... Disabled
External Policy Server.................. Disabled
Number of Active Clients................ 10
Exclusionlist........................... Disabled
Session Timeout......................... Infinity
Interface............................... management
DHCP Server............................. Disabled
Quality of Service...................... Gold (high)
Security
   802.11 Authentication:.................. Open System (Allow shared key)
   Static WEP Keys......................... Enabled
        Key Index:............................... 1
        Encryption:.............................. 104-bit WEP
   802.1X.................................. Disabled
   Wi-Fi Protected Access.................. Disabled
   Robust Secure Network................... Disabled
   IP Security............................. Disabled
   IP Security Passthru.................... Disabled
   L2TP.................................... Disabled
   Web Based Authentication................ Disabled
   Cranite Passthru........................ Disabled
   Fortress Passthru....................... Disabled
```

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, config wlan vlan

show wlan summary

To show a summary of the Cisco Wireless LAN Controller WLANs and their status, use the show wlan summary command.

>show wlan summary

Syntax

show	Display configurations.
wlan	Wireless LAN.
summary	Cisco Wireless LAN Controller Virtual Gateway IP Address.

Defaults (none)

Examples

```
>show wlan summary
WLAN ID WLAN Name              Status
------- ---------------------- ---------
1       Controller             Enabled
2       Marketing              Enabled
```

Related Commands config wlan summary

show wps signature summary

To show installed signatures of the Wireless Protection System (WPS) Peer Management, use the show wps signature summary command.

>show wps signature

Syntax

show	Display configurations.
wps	Wireless Protection System Peer Management.
signature summary	Installed signatures.

Defaults (none)

Example **>show wps signature summary**

```
Precedence..................................... 1
Signature Name................................. Bcast deauth
Type........................................... Standard
Frame Type..................................... Management
State.......................................... Enabled
Action......................................... report
Frequency...................................... 30 pkts/sec
Quiet Time..................................... 300 sec
Description.................................... Broadcast Deauthentication
Frame
  Patterns:
                    0:0x01:0xx01
                                          4:0x01:0x01.........................
--More-- or (q)uit
```

Related Commands config wps signature, config wps client-exclusion, config wps rogue-ap

show wps summary

To show a summary of the Wireless Protection System (WPS) Peer Management Configuration, use the show wps summary command.

>show wps summary

Syntax

show	Display configurations.
wps	Wireless Protection System Management.
summary	Summary of WPS manager.

Defaults (none)

Example **>show wps summary**

```
Client Exclusion Policy
   Excessive 802.11-association failures..................... Enabled
   Excessive 802.11-authentication failures.................. Enabled
   Excessive 802.1x-authentication........................... Enabled
   External policy server failure............................ Enabled
   IP-theft.................................................. Enabled
   Excessive Web authentication failure...................... Enabled

Trusted AP Policy
   Mis-configured AP Action.................................. Alarm Only
     Enforced encryption policy.............................. none
     Enforced preamble policy................................ none
     Enforced radio type policy.............................. none
     Validate SSID........................................... Disabled
```

```
   Alert if Trusted AP is missing.......................... Disabled
   Trusted AP timeout...................................... 120

Untrusted AP Policy
   Rogue Location Discover Protocol........................ Disabled
     RLDP Action........................................... Alarm Only
   Rogue APs
     Automatically contain rogues advertising.............. Alarm Only
     Detect Ad-Hoc Networks................................ Alarm Only
   Rogue Clients
     Validate rogue clients against AAA..................... Disabled
     Detect trusted clients on rogue APs.................... Alarm Only
   Rogue AP timeout........................................ 1200

Signature Policy
   Signature Processing.................................... Enabled
```

Related Commands config wps client-exclusion 802.11-auth, config wps client-exclusion 802.1x-auth, config wps client-exclusion all, config wps client-exclusion external-policy, config wps client-exclusion ip-theft, config wps client-exclusion web-auth, config wps rogue-ap aaa, config wps rogue-ap adhoc, config wps rogue-ap rldp, config wps rogue-ap ssid, config wps rogue-ap timeout, config wps rogue-ap valid-client, config wps rogue-ap encryption, config wps rogue-ap misconfigured-ap, config wps rogue-ap missing-ap, config wps rogue-ap preamble, config wps rogue-ap radio, config wps signature, show wps summary.

Setting Configurations

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

- *config 802.11a*
- *config 802.11b*
- *config aepi*
- *config acl*
- *config advanced 802.11a*
- *config advanced 802.11b*
- *config advanced client-handoff*
- *config advanced statistics*
- *config advanced timers*
- *config ap*
- *config exclusionlist*
- *config boot*
- *config certificate*
- *config client deauthenticate*
- *config country*
- *config custom-web*
- *config dhcp*
- *config known ap*
- *config interface*
- *config load-balancing*
- *config loginsession close*
- *config macfilter*
- *config mgmtuser*
- *config mirror*
- *config mobility*
- *config msglog level*
- *config netuser*
- *config network*
- *config port*
- *config prompt*
- *config qos queue_length*
- *config radius acct*
- *config radius auth*
- *config radius backward compatibility*

- *config radius callStationIdType*
- *config rogue ap*
- *config rogue adhoc*
- *config rogue client*
- *config route*
- *config serial*
- *config sessions*
- *config snmp community*
- *config snmp syscontact*
- *config snmp syslocation*
- *config snmp trapreceiver*
- *config snmp v3user*
- *config snmp version*
- *config spanning tree port*
- *config spanningtree switch*
- *config switchconfig*
- *config syslog*
- *config sysname*
- *config time*
- *config trapflags*
- *config watchlist*
- *config wlan*

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 address> <num of APs>

Syntax	config	Configure parameters.
	rogue ap	Rogue AP status.
	acknowledged	This AP has been identified and belongs to an external network.
	alert	This AP has not been identified. Generates a trap upon detection of this access point.
	contain	Start containing a rogue access point.
	known	This AP has been identified and is part of an internal network.
	<MAC address>	MAC address of the AP.
	<num of APs>	Number of APs.
Defaults	(none)	
Example	**>config rogue ap acknowledge 11:11:11:11:11:11**	

Related Commands • show rogue ap summary, show rogue ap detailed

CONFIG 802.11A COMMANDS

Use the following config 802.11a commands:

- *config 802.11a antMode*
- *config 802.11a beaconperiod*
- *config 802.11a channel*
- *config 802.11a disable*
- *config 802.11a dtim*
- *config 802.11a fragmentation*
- *config 802.11a enable*
- *config 802.11a fast-roaming*
- *config 802.11a pico-cell*
- *config 802.11a rate*
- *config 802.11a txPower*

config 802.11a antMode

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 antMode command.

```
>config 802.11a antMode <Cisco AP> <omni/sectorA/sectorB>
```

Syntax	config	Configure parameters.
	802.11a antMode	Antenna for 802.11a Cisco Radio.
	<Cisco AP>	Cisco 1000 Series IEEE 802.11a/b/g lightweight access point name.
	omni	Use both internal antennas.
	sectorA	Use only the Side A internal antenna.
	sectorB	Use only the Side B internal antenna.
Defaults	internal	
Examples	`>config 802.11a antMode AP1 omni`	
Related Commands	show ap config 802.11a, config 802.11b antMode	

config 802.11a beaconperiod

In Cisco SWAN 802.11a networks, all Cisco 1000 Series lightweight access point WLANs 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, be 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	config	Configure parameters.
	802.11a	802.11a network parameters.
	beaconperiod	Send a beacon every 100 to 600 milliseconds.
	<time units>	Beacon interval in milliseconds.
Defaults	100 milliseconds	
Examples	**>config 802.11a beaconperiod 120** to configure an 802.11a network for a beacon period of 120 milliseconds.	
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 1000 Series light-weight access point> <global/channel #>}

Syntax	config	Configure parameters.
	802.11a channel	Cisco Radio channel number.
	global	Global channel control.
	<Cisco 1000 Series lightweight access point>	Name of Cisco 1000 Series light-weight access point or global setting for all Cisco 1000 Series lightweight access points.
Defaults	(none)	
Examples	To have Radio Resource Management (RRM) automatically configure all 802.11a channels based on availability and interference: **>config 802.11a channel global auto** To have Radio Resource Management (RRM) automatically reconfigure all 802.11a channels one time based on availability and interference: **>config 802.11a channel global once** To turn 802.11a Radio Resource Management (RRM) automatic configuration off: **>config 802.11a channel global off** To configure all 802.11a channels in AP1: **>config 802.11a channel AP1 global** To configure 802.11a channel 36 in AP1: **>config 802.11a channel AP1 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, use the config 802.11a disable command.

Disable 802.11a transmissions for the whole network or for an individual Cisco Radio using the config 802.11a disable command.

Note that you must use this command to disable the network before using many config 802.11a commands.

This command can be used any time the CLI interface is active.

```
>config 802.11a disable {network/<Cisco 1000 Series lightweight access
point>}
```

Syntax

config	Configure parameters.
802.11a	802.11a network parameters.
disable	Disable 802.11a.
network	Whole network.
<Cisco 1000 Series lightweight access point>	Override the network setting for an individual <Cisco 1000 Series lightweight access point> Cisco Radio.

Defaults Network = enabled.

Examples To disable the whole 802.11 a network:

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

To disable AP1 802.11a transmissions:

```
>config 802.11a disable AP1
```

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 WLANs 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 <value>

Syntax	config	Configure parameters.
	802.11a	802.11a network parameters.
	dtim	Delivery Traffic Indication Map.
	<value>	DTIM value in number of beaconperiods.
Defaults	1 (every beaconperiod)	
Examples	**>config 802.11a dtim 2** to configure the 802.11a network to transmit multicast and broadcast messages every other DTIM, or beaconperiod.	
Related Commands	show 802.11a, config 802.11a beaconperiod, config 802.11b 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 operational.

>config 802.11a fragmentation <threshold>}

Syntax	config	Configure parameters.
	802.11a	802.11a network parameters.
	fragmentation	Fragmentation threshold.
	<threshold>	Fragmentation threshold value.
Defaults	None.	
Example	**>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 SWAN 802.11a network. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual WLAN, use the config wlan radio command.

This command can be used any time the CLI interface is active.

>config 802.11a enable {network/<Cisco 1000 Series lightweight access point>}

Syntax	config	Configure parameters.
	802.11a	802.11a network parameters.
	enable	Enable 802.11a.

	network	For the whole network.
	<Cisco 1000 Series lightweight access point>	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 fast-roaming

To configure the 802.11a fast roaming extensions, use the config 802.11a fast-roaming command.

>config 802.11a fast-roaming <enable/disable/voip-minrate{AP mac address/1, 2, 5.5, 11 Mbps}/voip-percentage{0, 25, 50, or 100}>}

Syntax	config	Configure parameters.
	802.11a	802.11a network parameters.
	fast-roaming	Fast roaming feature.
	<enable/disable>	Enable or disable.
	voip-minrate	Voice over internet AP mac address and rate
	voip-percentage	Voice over internet percentage

Defaults (None.)

Examples **>config 802.11a fast-roaming enable**
>config 802.11a fast-roaming voip-percentage 50

Related Commands config 802.11b fast-roaming, config 802.11a fast-roaming, show 802.11a

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	config	Configure parameters.
	802.11a	802.11a network parameters.
	pico-cell	Pico cell extensions.
	<enable/disable>	Enable or disable.

Defaults (None.)

Example **>config 802.11a pico-cell <enable/disable>**

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.

Note: 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	config	Configure parameters.
	802.11a	802.11a network parameters.
	rate	Data rate.
	disabled/mandatory/supported	See Note above.
	rate	6000, 9000, 12000, 18000, 24000, 36000, 48000, or 54000 Kbps.
Defaults	(none)	
Examples	To set 802.11a transmission at a mandatory rate at 12000 Kbps: **>config 802.11a rate mandatory 12000**	
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/power level #>}/{<AP Name> <global/
power level #>}
```

Syntax	config	Configure parameters.
	802.11a	802.11a network parameters.
	txPower	Transmit power parameter.
	global	All Cisco 1000 Series lightweight access points.
	auto	Periodic Radio Resource Management (RRM) automatic configuration.
	<AP Name>	Cisco 1000 Series IEEE 802.11a/b/g lightweight access point name.
	power level #	Transmit power level number.

Note: The 802.11a Cisco Radio supports five transmit power levels: 1 = Maximum transmit power level allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

Refer to Cisco SWAN Supported Country Codes in the Product Guide for the maximum regulatory Transmit Power Level Limits published for each Country Code. Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Also note that the actual maximum transmit power levels may be less than the published regulatory limits.

Defaults Global, Auto.

Examples To have Radio Resource Management (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 (lowest):
>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 following config 802.11b command:

- *config 802.11b 11gSupport*
- *config 802.11b antenna*
- *config 802.11b beaconperiod*
- *config 802.11b channel*
- *config 802.11b disable*
- *config 802.11b diversity*
- *config 802.11b dtim*
- *config 802.11b fragmentation*
- *config 802.11b enable*
- *config 802.11b fast-roaming*
- *config 802.11b pico-cell*
- *config 802.11b preamble*
- *config 802.11b rate*
- *config 802.11b txPower*

config 802.11b 11gSupport

After enabling the Cisco SWAN 802.11b network using the config 802.11b enable command, enable or disable the Cisco SWAN 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 SWAN 802.11g network after the Cisco SWAN 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 WLAN, 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	config	Configure parameters.
	802.11b	802.11b network parameters.
	11gSupport	Support for the 802.11g network.
	enable/disable	Enable or disable 802.11b/g.
	<Cisco 1000 Series lightweight access point>	To override the network setting for individual <Cisco 1000 Series lightweight access point> Cisco Radio.

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

To configure the 802.11b/g antenna, use the config 802.11b antenna command.

Use the config 802.11b disable command to disable the 802.11b/g Cisco Radio before using the config 802.11b antenna command. Then use the config 802.11b antenna command to configure the Cisco 1000 Series lightweight access point to use internal or external antennas. Then use the config 802.11b enable command to enable the 802.11b/g Cisco Radio.

```
>config 802.11b antenna <Cisco 1000 Series lightweight access point>
<internal/external>
```

Syntax	config	Configure parameters.
	802.11b antenna	Antennas for 802.11b/g Cisco Radio.
	<Cisco 1000 Series lightweight access point>	Cisco 1000 Series lightweight access point name.
	<internal/external>	Configure for internal or external antennas.

Defaults Internal.

Examples

```
>config 802.11b antenna AP1 internal
```

to set AP1 to use the 802.11b/g internal antennas.

Related Commands config 802.11b disable, config 802.11b enable, config 802.11a antMode

config 802.11b beaconperiod

In Cisco SWAN 802.11b/g networks, all Cisco 1000 Series lightweight access point WLANs 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, be sure that you have disabled the 802.11b/g network using the config 802.11b disable command. When you are done changing the beacon period, remember to enable the 802.11b/g network using the config 802.11b enable command.

```
>config 802.11b beaconperiod <Time Units>
```

Syntax	config	Configure parameters.
	802.11b	802.11b/g network parameters.
	beaconperiod	Send a beacon every 100 to 600 milliseconds.
	<time units>	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 Radio Resource Management (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 1000 Series lightweight access point> <global/channel #>}

Syntax	config	Configure parameters.
	802.11b channel	802.11b/g Cisco Radio channel number.
	global	Global channel control.
	<Cisco 1000 Series lightweight access point>	Name of Cisco 1000 Series lightweight access point or global setting for all Cisco 1000 Series lightweight access points.
Defaults	(none)	
Examples	To have Radio Resource Management (RRM) automatically configure all 802.11b/g channels based on availability and interference: **>config 802.11b channel global auto** To have Radio Resource Management (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 Radio Resource Management (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**	

Note: 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 <enable/disable>{network/<Cisco 1000 Series light-weight access point>}

Syntax

config	Configure parameters.
802.11b	802.11b/g network parameters.
disable	Disable 802.11b/g.
enable/disable	Enable or disable.
network	Whole network.
<Cisco 1000 Series lightweight access point>	Override the network setting for an individual <Cisco 1000 Series lightweight access point> Cisco Radio.

Defaults Enabled.

Examples **>config 802.11b disable network**
to disable the whole 802.11b/g network.

>config 802.11b disable AP1
to disable AP1 802.11b/g transmissions.

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 diversity

To configure the diversity option for 802.11b/g antennas, use the config 802.11b diversity command.

>config 802.11b diversity <Cisco 1000 Series lightweight access point> <enable/sideA/sideB>

Syntax

config	Configure parameters.
802.11b diversity	Diversity antennas for 802.11b/g.
<Cisco 1000 Series lightweight access point>	Cisco 1000 Series lightweight access point name.
enable	Between the two internal antennas.
sideA	Between the internal antennas and an external antenna connected to the Cisco 1000 Series light-weight access point Left port.
sideB	Between the internal antennas and an external antenna connected to the Cisco 1000 Series light-weight access point Right port.

Defaults Enabled.

Examples To enable diversity for AP1:

>**config 802.11b diversity AP1 enable**

To enable diversity for AP1 using an external antenna connected to the Cisco 1000 Series lightweight access point Left port (sideA).
>**config 802.11b diversity AP1 sideA**

Related Commands show ap config 802.11b

config 802.11b dtim

In 802.11 networks, the Cisco 1000 Series lightweight access point WLANs broadcast a beacon at regular intervals, which coincide 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 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, be 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		
	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 >**config 802.11b dtim 1**
to configure the 802.11b/g network to transmit multicast and broadcast messages every DTIM, or beaconperiod.

Related Commands show 802.11b, config 802.11b beaconperiod, config 802.11a 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	config	Configure parameters.
	802.11b	802.11b network parameters.
	fragmentation	Fragmentation threshold.
	<threshold>	Fragmentation threshold value.
Defaults	None.	
Example	**>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 SWAN 802.11b network. To enable the Cisco SWAN 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 WLAN, 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 1000 Series lightweight access point>}

Syntax	config	Configure parameters.
	802.11b	802.11b network parameters.
	enable	Enable 802.11b. Allow support for 802.11g.
	network	For the whole network.
	<Cisco 1000 Series lightweight access point>	To override the network setting for individual <Cisco 1000 Series lightweight access point> Cisco Radio.
Defaults	Enabled.	
Examples	**>config 802.11b enable network** to enable the whole 802.11b network and provide support for the 802.11g network.	
	>config 802.11b enable AP1 to enable AP1 802.11b transmissions and support AP1 802.11g transmissions.	
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 fast-roaming

To configure the 802.11b/g fast roaming extensions, use the config 802.11b fast-roaming command.

```
>config 802.11b fast-roaming <enable/disable/voip-minrate{AP mac address/1,
2, 5.5, 11 Mbps}/voip-percentage{0, 25, 50, or 100}>}
```

Syntax	config	Configure parameters.
	802.11ab	802.11ab network parameters.
	fast-roaming	Fast roaming feature.
	<enable/disable>	Enable or disable.
	voip-minrate	Voice over internet AP mac address and rate
	voip-percentage	Voice over internet percentage

Defaults (None.)

Examples
```
>config 802.11b fast-roaming enable
>config 802.11b fast-roaming voip-percentage 50
```

Related Commands config 802.11a fast-roaming, show 802.11b

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	config	Configure parameters.
	802.11b	802.11b network parameters.
	pico-cell	Pico cell extensions.
	<enable/disable>	Enable or disable.

Defaults (None.)

Example
```
>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 that you must reboot the Cisco Wireless LAN Controller (reset system) with save to implement this command.

```
>config 802.11b preamble [short/long]
```

Syntax	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>
```

Note: 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

config	Configure parameters.
802.11b	802.11b/g network parameters.
disabled/mandatory/supported	See the Note above.
rate	1, 2, 5.5, or 11 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/powerLevel #>}/{<Cisco 1000 Series
lightweight access point> <global/powerLevel #>}
```

Syntax

config	Configure parameters.
802.11b	802.11b/g network parameters.
txPower	Transmit power parameter.
global	All Cisco 1000 Series lightweight access points.
auto/	Periodic Radio Resource Management (RRM) automatic configuration.
<Cisco 1000 Series lightweight access point>	Cisco 1000 Series IEEE 802.11a/b/g lightweight access point name.
power level #	Transmit power level number.

Note: The Cisco 1000 Series lightweight access point 802.11b Cisco Radio supports five transmit power levels: 1 = Maximum transmit power level allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

Refer to Cisco SWAN Supported Country Codes in the Product Guide for the maximum regulatory Transmit Power Level Limits published for each Country Code. Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Also note that the actual maximum transmit power levels may be less than the published regulatory limits.

Defaults Global, Auto.

Examples To have Radio Resource Management (RRM) automatically set the transmit power for all 802.11b/g Cisco Radios at periodic intervals:
>config 802.11a txPower global auto

To have Radio Resource Management (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 (lowest):
>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 aepi

To configure External Policy Servers, use the config aepi command.

>config aepi [acl/add/delete/disable/enable] [index]

Syntax

config aepi	Command action.
acl	Configures the AEPI ACL Name.
add <index> <IP addr> <port> <secret>	Configures the External Policy Server.
delete <index>	Deletes the External Policy Server.
disable <index>	Disables the External Policy Server.
enable <index>	Enables the External Policy Server.

Defaults N/A

Examples **>config aepi enable acl01**

Related Commands show aepi

config acl

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

>config acl [apply/create/delete/rule] [name]

Syntax	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	Configure rules in the ACL.
	Name	ACL name.
Defaults	N/A	
Examples	**>config acl create acl01**	
Related Commands	show acl	

CONFIG ADVANCED 802.11A COMMANDS

Use the following advanced 802.11a commands:

- *config advanced 802.11a channel foreign*
- *config advanced 802.11a channel load*
- *config advanced 802.11a channel noise*
- *config advanced 802.11a channel update*
- *config advanced 802.11a factory*
- *config advanced 802.11a group-mode*
- *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 txpower*
- *config advanced 802.11a monitor coverage*
- *config advanced 802.11a monitor load*
- *config advanced 802.11a monitor mode*
- *config advanced 802.11a monitor noise*
- *config advanced 802.11a monitor signal*
- *config advanced 802.11a receiver*
- *config advanced 802.11a txpower-update*
- *config advanced 802.11a profile clients*
- *config advanced 802.11a profile coverage*
- *config advanced 802.11a profile customize*
- *config advanced 802.11a profile exception*
- *config advanced 802.11a profile foreign*

- *config advanced 802.11a profile level*
- *config advanced 802.11a profile noise*
- *config advanced 802.11a profile throughput*
- *config advanced 802.11a profile utilization*

config advanced 802.11a channel foreign

To have Radio Resource Management (RRM) consider or ignore foreign 802.11a interference 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	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	channel	Radio Resource Management (RRM) channel selections.
	foreign	Foreign interference.
	[enable/disable]	Consider or ignore.

Defaults Enabled.

Examples **>config advanced 802.11a channel foreign enable**
to have Radio Resource Management (RRM) consider foreign 802.11a interference when making channel selection updates for all 802.11a Cisco 1000 Series lightweight access points.

Related Commands show advanced 802.11a channel, config advanced 802.11b channel foreign

config advanced 802.11a channel load

To have Radio Resource Management (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	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	channel	Radio Resource Management (RRM) channel selections.
	load	Traffic load.
	[enable/disable]	Consider or ignore.

Defaults Disabled.

Examples **>config advanced 802.11a channel load enable**
to have Radio Resource Management (RRM) consider traffic load when making channel selection updates for all 802.11a Cisco 1000 Series lightweight access points.

Related Commands show advanced 802.11a channel, config advanced 802.11b channel load

config advanced 802.11a channel noise

To have Radio Resource Management (RRM) consider or ignore non-802.11a noise in making channel selection updates for all 802.11a Cisco 1000 Series lightweight access points, use the config advanced 802.11a channel noise command.

>config advanced 802.11a channel noise [enable/disable]

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	channel	Radio Resource Management (RRM) channel selections.
	noise	Non-802.11a noise.
	[enable/disable]	Consider or ignore.

Defaults Disabled.

Examples **>config advanced 802.11a channel noise enable**
to have Radio Resource Management (RRM) consider non-802.11a noise when making channel selection updates for all 802.11a Cisco 1000 Series lightweight access points.

Related Commands show advanced 802.11a channel, config advanced 802.11b channel noise

config advanced 802.11a channel update

To have Radio Resource Management (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	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	channel update	Have Radio Resource Management (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	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	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	group-mode	Cisco Radio RF grouping.
	auto/off	Sets to automatic or disables.
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	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	logging channel	Log channel changes.
	<on/off>	Enable or Disable 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 channel change logging mode on or off, use the config advanced 802.11a logging channel command.

>config advanced 802.11a logging coverage <on/off>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	logging coverage	Log coverage changes.
	<on/off>	Enable or Disable 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 channel change logging mode on or off, use the config advanced 802.11a logging channel command.

>config advanced 802.11a logging foreign <on/off>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	logging foreign	Log foreign changes.
	<on/off>	Enable or Disable 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 channel change logging mode on or off, use the config advanced 802.11a logging channel command.

>config advanced 802.11a logging load <on/off>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	logging load	Log load changes.
	<on/off>	Enable or Disable 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 channel change logging mode on or off, use the config advanced 802.11a logging channel command.

>config advanced 802.11a logging noise <on/off>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	logging noise	Log noise changes.
	<on/off>	Enable or Disable 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 channel change logging mode on or off, use the config advanced 802.11a logging performance command.

>config advanced 802.11a logging performance <on/off>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	logging performance	Log performance changes.
	<on/off>	Enable or Disable 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 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	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	logging txpower	Log power changes.
	<on/off>	Enable or disable 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 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	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	monitor coverage	Monitor coverage interval.
	<seconds>	60 to 3600 seconds.
Defaults	180 seconds.	
Examples	>**config advanced 802.11a monitor coverage 60** to set the coverage measurement interval to 60 seconds.	
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	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.

	monitor load	Monitor load interval.
	<seconds>	60 to 3600 seconds.

Defaults 60 seconds.

Examples >**config advanced 802.11a monitor load 60**
to set the load measurement interval to 60 seconds.

Related Commands show advanced 802.11a monitor, config advanced 802.11b monitor load

config advanced 802.11a monitor mode

To enable or disable the 802.11a monitor mode, use the config advanced 802.11a monitor mode command.

>config advanced 802.11a monitor mode <enable/disable>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	monitor mode	Monitor mode.
	<enable/disable>	Enable or disable.

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 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	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	monitor noise	Monitor noise interval.
	<seconds>	60 to 3600 seconds

Defaults 180 seconds.

Examples >**config advanced 802.11a monitor noise 120**
to set the noise measurement interval to 120 seconds.

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	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	monitor signal	Monitor signal interval.
	<seconds>	60 to 3600 seconds

Defaults 60 seconds.

Examples >**config advanced 802.11a monitor signal 120**
to set the signal measurement interval to 120 seconds.

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		
	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	receiver	Receiver configuration.
	<default/rxstart>	default configuration/start configuration

Defaults (None)

Examples >**config advanced 802.11a receiver default**
Cannot change receiver params while network is enabled

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		
	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 1000 Series light-weight access point> <value>**

Syntax		
	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile clients	Cisco 1000 Series lightweight access point Client profile
	global/<Cisco 1000 Series	lightweight access point>global or Cisco 1000 Series lightweight access point specific profile.
	<value>	1 to 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

To set the AP1 clients threshold to 75 clients:
>config advanced 802.11a profile clients AP1 75

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 1000 Series light-weight access point> <value>

Syntax		
	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile coverage	Cisco 1000 Series lightweight access point profile coverage
	global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile.
	<value>	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 1000 Series lightweight access point> <on|off>

Syntax		
	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	customize	Performance profile.
	Cisco 1000 Series lightweight access point	Cisco 1000 Series lightweight access point.
	on/off	Enable or disable.

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 1000 Series light-weight access point> <value>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile exception	Cisco 1000 Series lightweight access point profile exception
	global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile.
	<value>	0 to 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 1000 Series light-weight access point>} <value>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile foreign	foreign interference profile.
	global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile.
	<value>	0 to 100 percent.

Defaults 10 percent.

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 1000 Series lightweight access point> <value>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile level	Cisco 1000 Series lightweight access point profile level
	global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile.
	<value>	1 to 75 clients.
Defaults	3 clients.	
Examples	>**config advanced 802.11a profile level global 10** to set all Cisco 1000 Series lightweight access point client minimum exception levels to 10 clients. >**config advanced 802.11a profile level AP1 25** to set the AP1 client minimum exception level to 25 clients.	
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 1000 Series lightweight access point> <value>**

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile noise	Profile noise limits
	global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile.
	<value>	-127 to 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 1000 Series light-
weight access point>} <value>
```

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile throughput	Data rate threshold
	global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile.
	<value>	1,000 to 10,000,000 bps.

Defaults 1,000,000 bps.

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 1000 Series light-
weight access point> <value>
```

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile utilization	Cisco 1000 Series lightweight access point profile utilization
	global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile.
	<value>	0 to 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 following config advanced 802.11b commands:

- *config advanced 802.11b channel foreign*
- *config advanced 802.11b channel load*
- *config advanced 802.11b channel noise*
- *config advanced 802.11b channel update*

- *config advanced 802.11b factory*
- *config advanced 802.11b group-mode*
- *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 txpower*
- *config advanced 802.11b monitor channel-list*
- *config advanced 802.11b monitor coverage*
- *config advanced 802.11b monitor load*
- *config advanced 802.11b monitor mode*
- *config advanced 802.11b monitor noise*
- *config advanced 802.11b monitor signal*
- *config advanced 802.11b receiver*
- *config advanced 802.11b txpower-update*
- *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*

config advanced 802.11b channel foreign

To have Radio Resource Management (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	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	channel	Radio Resource Management (RRM) channel selections.
	foreign	Foreign interference.
	[enable/disable]	Consider or ignore.

Defaults Enabled.

Examples >**config advanced 802.11b channel foreign enable**
to have Radio Resource Management (RRM) consider foreign 802.11b/g interference when making channel selection updates for all 802.11b/g Cisco 1000 Series lightweight access points.

Related Commands show advanced 802.11b channel, config advanced 802.11a channel foreign

config advanced 802.11b channel load

To have Radio Resource Management (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		
	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	channel	Radio Resource Management (RRM) channel selections.
	load	Traffic load.
	[enable/disable]	Consider or ignore.

Defaults Disabled.

Examples >**config advanced 802.11b channel load enable**
to have Radio Resource Management (RRM) consider traffic load when making channel selection updates for all 802.11b/g Cisco 1000 Series lightweight access points.

Related Commands show advanced 802.11b channel, config advanced 802.11a channel load

config advanced 802.11b channel noise

To have Radio Resource Management (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		
	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	channel	Radio Resource Management (RRM) channel selections.
	noise	Non-802.11b/g noise.
	[enable/disable]	Consider or ignore.

Defaults Disabled.

Examples >**config advanced 802.11b channel noise enable**
to have Radio Resource Management (RRM) consider non-802.11b/g noise when making channel selection updates for all 802.11b/g Cisco 1000 Series lightweight access points.

Related Commands show advanced 802.11b channel, config advanced 802.11a channel noise

config advanced 802.11b channel update

To have Radio Resource Management (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	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	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	**>config advanced 802.11b factory** to reset all 802.11b/g advanced settings back to the factory defaults.	
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	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	group-mode	Cisco Radio RF grouping.
	<auto/off>	Automatic selection or off.
Defaults	Auto.	
Usage	Use to enable or disable 802.11b/g automatic RF group selection mode.	
Examples	**>config advanced 802.11b group-mode auto** to set the 802.11b/g RF group selection mode to automatic. **>config advanced 802.11b group-mode off** to disable the 802.11b/g RF group selection mode.	
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	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	logging channel	Log channel changes.
	<on/off>	Enable or Disable 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 channel change logging mode on or off, use the config advanced 802.11b logging channel command.

>config advanced 802.11b logging coverage <on/off>

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	logging coverage	Log coverage changes.
	<on/off>	Enable or Disable 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 channel foreign logging mode on or off, use the config advanced 802.11b logging foreign command.

>config advanced 802.11b logging foreign <on/off>

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	logging foreign	Log foreign changes.
	<on/off>	Enable or Disable logging
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 channel load logging mode on or off, use the config advanced 802.11b logging load command.

>config advanced 802.11b logging load <on/off>

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	logging load	Log load changes.
	<on/off>	Enable or Disable 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 channel noise logging mode on or off, use the config advanced 802.11b logging noise command.

>config advanced 802.11b logging noise <on/off>

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	logging noise	Log noise changes.
	<on/off>	Enable or Disable 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 channel performance logging mode on or off, use the config advanced 802.11b logging performance command.

>config advanced 802.11b logging performance <on/off>

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	logging performance	Log performance changes.
	<on/off>	Enable or Disable 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 logging mode on or off, use the config advanced 802.11b logging txpower command.

>config advanced 802.11b logging txpower <on/off>

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	logging txpower	Log power changes.

	<on/off>	Enable or Disable 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	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	monitor channel-list	Monitor channel list.
	<all/	Monitor all channels
	country/	Monitor channels used in configured country code
	dca>	Monitor channels used by automatic channel assignment

Defaults 180 seconds.

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	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	monitor coverage	Monitor coverage interval.
	<seconds>	60 to 3600 seconds.

Defaults 180 seconds.

Examples **>config advanced 802.11b monitor coverage 60**
to set the coverage measurement interval to 60 seconds.

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	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	monitor load	Monitor load interval.

	<seconds>	60 to 3600 seconds

Defaults 60 seconds.

Examples **>config advanced 802.11b monitor load 60**
to set the load measurement interval to 60 seconds.

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	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b parameters.
	monitor mode	Monitor mode.
	<enable/disable>	Enable or disable.

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	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	monitor noise	Monitor noise interval.
	<seconds>	60 to 3600 seconds

Defaults 180 seconds.

Examples **>config advanced 802.11b monitor noise 120**
to set the noise measurement interval to 120 seconds.

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	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	monitor signal	Monitor signal interval.
	<seconds>	60 to 3600 seconds

Defaults 60 seconds.

Examples **>config advanced 802.11b monitor signal 120**
to set the signal measurement interval to 120 seconds.

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		
	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b parameters.
	receiver	Receiver configuration.
	<default/rxstart>	default configuration/start configuration

Defaults (None)

Examples **>config advanced 802.11b receiver default**
Cannot change receiver params while network is enabled

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		
	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 1000 Series light-weight access point> <value>

Syntax		
	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	profile clients	Client profiles.
	global/<Cisco 1000 Series lightweight access point>	Global or Cisco 1000 Series lightweight access point specific profile.
	<value>	1 to 75 clients.

Defaults 12 clients

Examples **>config advanced 802.11b profile clients global 25**

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

>config advanced 802.11b profile clients AP1 75
to set the Cisco 1000 Series lightweight access point clients threshold for AP1 to 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 1000 Series light-weight access point> <value>

Syntax

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
profile coverage	Cisco 1000 Series lightweight access point profile coverage
global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile
<value>	3 to 50 dB

Defaults 12 dB

Examples **>config advanced 802.11b profile coverage global 30**
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 AP1 50
to set the Cisco 1000 Series lightweight access point coverage threshold for AP1 to 50 dB.

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 1000 Series lightweight access point> <on|off>

Syntax

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.

Defaults Off

Example: **>config advanced 802.11b profile customize on**
to turn customization on for the AP1 performance profile.

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 1000 Series light-weight access point> <value=0 to 100 percent>

Syntax

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
profile exception	Cisco 1000 Series lightweight access point profile exception
global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile
<value>	0 to 100 percent

Defaults 25%

Examples **>config advanced 802.11b profile exception global 0**
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 AP1 100
to set the Cisco 1000 Series lightweight access point coverage exception level for AP1 to 100 percent.

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 1000 Series light-weight access point>} <value> (0 to 100 percent)

Syntax

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
profile foreign	foreign interference profile.
global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile.
<value>	0 to 100 percent.

Defaults 802.11b/g foreign profile = (tbd) percent.

Examples **>config advanced 802.11b profile foreign global 50**
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 AP1 0
to set the foreign 802.11b/g transmitter interference threshold for AP1 to 0 percent.

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 1000 Series lightweight access point> <value>

Syntax

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
profile minimum	Cisco 1000 Series lightweight access point profile level
global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile
<value>	1 to 75 clients

Defaults 3 clients

Examples **>config advanced 802.11b profile level global 75**
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 AP1 25
to set the Cisco 1000 Series lightweight access point client minimum exception level for AP1 to 25 clients.

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 1000 Series lightweight access point> <value>

Syntax

config	Configure parameters.
advanced 802.11b	Advanced 802.11b/g parameters.
profile noise	Cisco 1000 Series lightweight access point profile noise
global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile
<value>	-127 to 0 dBm

Defaults -70 dB

Examples **>config advanced 802.11b profile noise global -90**
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 AP1 -30
to set the 802.11b/g foreign noise threshold for AP1 to -30 dBm.

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 1000 Series light-weight access point> <value>

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	profile throughput	Throughput profile.
	global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile.
	<value>	1,000 to 10,000,000 bps.
Defaults	1,000,000 bps	
Examples	**>config advanced 802.11b profile throughput global 1000** 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 AP1 10000000 to set the Cisco 1000 Series lightweight access point throughput threshold for AP1 to 10000000 bytes per second.	
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 1000 Series light-weight access point> <value>

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	profile utilization	Cisco 1000 Series lightweight access point profile utilization
	global/<Cisco 1000 Series lightweight access point>	global or Cisco 1000 Series lightweight access point specific profile
	<value>	0 to 100 percent
Defaults	80%	
Examples	**>config advanced 802.11b profile utilization global 100** to set the RF utilization threshold for the whole 802.11b/g network to 100 percent.	
	>config advanced 802.11b profile utilization AP1 50 to set the RF utilization threshold for the AP1 to 50 percent.	
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 <value = 0-255>

Syntax	config	Configure parameters.
	advanced	Advanced parameters.
	client-handoff <value>	0 to 255 excessive retries before client handoff.
Defaults	0 excessive retries (disabled).	
Examples	>**config advanced client-handoff 100** to set the client handoff to 100 excessive retries.	
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	config	Configure parameters.
	advanced	Advanced parameters.
	statistics	Statistics.
	<enable/disable>	Enable or disable statistics.
Defaults	Enabled.	
Examples	>**config advanced statistics disable** to disable statistics.	
Related Commands	show advanced statistics, show stats port, show stats switch	

CONFIG ADVANCED TIMERS COMMANDS

User the following config advanced timers commands:

- *config advanced timers ap-discovery-timeout*
- *config advanced timers ap-heartbeat-timeout*
- *config advanced timers auth-timeout*
- *config advanced timers eap-timeout*

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 an unconnected Cisco 1000 Series lightweight access point. 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	config	Configure parameters.
	advanced	Advanced parameters.
	timers	Network timers.
	ap-discovery-timeout	Cisco 1000 Series lightweight access point discovery timeout.
	<seconds>	Timeout period 1-10 seconds.

Defaults 10 seconds.

Example **>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		
	config	Configure parameters.
	advanced	Advanced parameters.
	timers	Network timers.
	ap-heartbeat-timeout	Cisco 1000 Series lightweight access point heartbeat timeout.
	<seconds>	Timeout period 1-30 seconds.

Defaults 30 seconds.

Example **>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		
	config	Configure parameters.
	advanced	Advanced parameters.
	timers	Network timers.
	auth-timeout	Authentication response timeout.
	<seconds>	Timeout period in seconds.

Defaults 10 seconds.

Example **>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. U

>config advanced timers eap-timeout <seconds>

Syntax		
	config	Configure parameters.
	advanced	Advanced parameters.
	timers	Network timers.
	eap-timeout	EAP timeout.
	<seconds>	Timeout period in seconds between 8 and 60.

Defaults (None.)

Example `>config advanced timers eap-timeout 10`

Related Commands show advanced timers

CONFIG AP COMMANDS

Use the following config ap commands:

- *config ap add*
- *config ap delete*
- *config ap disable*
- *config ap enable*
- *config ap get-crash-data*
- *config ap location*
- *config ap mode*
- *config ap name*
- *config ap port*
- *config ap primary-base*
- *config ap remote-debug*
- *config ap reporting-period*
- *config ap reset*
- *config ap stats-timer*
- *config ap secondary-base*
- *config ap tertiary-base*
- *config ap static-ip*
- *config ap wlan*

config ap add

To add a Third-Party access point, use the config ap add command. This command only applies to Third-Party APs, as Cisco 1000 Series lightweight access points are automatically detected and added to the Cisco Wireless LAN Controller.

`>config ap add <MAC address> <port> [enable/disable] <ip-addr>`

Syntax		
	config	Configure parameters.
	ap	Access point.
	add	Add a Third-Party AP.
	<MAC address>	MAC address of the Third-Party AP.
	<port>	Port number of the Cisco Wireless LAN Controller where AP is connected.
	[enable/disable]	Enable or disable the port
	<ip-addr>	IP address

Defaults (none)

Example >**config ap add ac:10:02:72:2f:bf 12**

Related Commands config 802.11a antenna, config 802.11b antenna

config ap delete

To delete a Third-Party access point from the Cisco Wireless LAN Controller, use the config ap delete command.

>config ap delete <MAC address>

Syntax	config	Configure parameters.
	ap	Access point.
	delete	Delete a Third-Party AP.
	<MAC address>	MAC address of the Third-Party AP.

Defaults (none)

Examples >**config ap delete ac:10:02:72:2f:bf**

Related Commands config 802.11a antenna, config 802.11b antenna

config ap disable

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

>config ap disable <Cisco 1000 Series lightweight access point>

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	disable	Disable command.
	<Cisco 1000 Series lightweight access point>	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 1000 Series lightweight access point>

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

Defaults (none)

Examples >**config ap enable AP1**

Related Commands config ap disable

config ap get-crash-data

To collect the latest crash data for a Cisco 1000 Series lightweight access point, use the config ap get-crash-data command. Use the *transfer upload datatype* command to transfer the collected data to the Cisco Wireless LAN Controller.

>config ap get-crash-data <Cisco 1000 Series lightweight access point>

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	get-crash-data	Enable command.
	<Cisco 1000 Series lightweight access point>	Name of the Cisco 1000 Series lightweight access point.
Defaults	(none)	
Examples	>**config ap get-crash-data AP3**	

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 1000 Series lightweight access point>

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	location	Descriptive location.
	"<location>"	Location name (enclosed by double quotation marks).
	<Cisco 1000 Series lightweight access point>	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 edge, must connect to a Cisco 1030 remote edge light-weight 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.

>config ap mode [local/reap/monitor/rogue] <Cisco 1000 Series lightweight access point>

Syntax	config ap mode	Configure boot option.
	local/reap/monitor/rogue	Set the Cisco 1000 Series lightweight access point for local (normal), reap (remote edge), monitor (listen-only) or rogue mode.
	<Cisco 1000 Series lightweight access point>	Name of the Cisco 1000 Series lightweight access point.
Defaults	Local.	

Examples

>config ap mode local AP01
sets the Cisco Wireless LAN Controller to communicate with AP01 in local (normal) mode.

>config ap mode reap AP91
sets the Cisco Wireless LAN Controller to communicate with Cisco 1030 remote edge lightweight access point AP91 in remote edge mode.

>config ap mode monitor AP02
sets the Cisco Wireless LAN Controller to communicate with AP02 in monitor (listen-only) mode.

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 AP name> <Old AP name>

Syntax

config	Configure parameters.
ap	Cisco 1000 Series lightweight access point.
name	Name of the Cisco 1000 Series lightweight access point.
<New AP name>	Desired Cisco 1000 Series lightweight access point name.
<Old AP 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 of a Third-Party access point, use the config ap port command.

>config ap port <MAC address> <port> [enable/disable] <ip-addr>

Syntax

config	Configure parameters.
ap	Access point.
<MAC address>	MAC address of the Third-Party AP.
port	Cisco Wireless LAN Controller port.
[enable/disable]	Enable or disable the port.
<ip-addr>	IP address.

Defaults (none)

Examples **>config ap port ac:10:02:72:2f:bf**

Related Commands show ap config

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 1000 Series lightweight access point>

Syntax	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 1000 Series lightweight access point>	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] (command) <Cisco 1000 Series lightweight access point>

Syntax	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]	Enable or disable remote debugging of a Cisco 1000 Series lightweight access point, or remotely execute a command.
	(command)	Optional command to be executed.
	<Cisco 1000 Series lightweight access point>	Cisco 1000 Series lightweight access point name.
Defaults	Disabled.	
Examples	**>config ap remote-debug enable AP01** to enable remote debugging on AP01. **>config ap remote-debug disable AP02** to disable remote debugging on AP02. **>config ap remote-debug exc-command (command) AP03** to execute Cisco Technical Assistance Center (TAC)-provided commands on 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	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)	
Example	>**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 1000 Series lightweight access point>

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	reset	Reset command.
	<Cisco 1000 Series lightweight access point>	Cisco 1000 Series lightweight access point name.
Defaults	(none)	
Example	>**config ap reset AP2**	
Related Commands	show ap config	

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 1000 Series lightweight access point>

Syntax	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.
	<Cisco 1000 Series lightweight access point>	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 1000 Series lightweight access point>

Syntax	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 1000 Series lightweight access point>	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 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 1000 Series lightweight access point>

Syntax	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 1000 Series lightweight access point>	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 static-ip

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

>config ap static-ip [enable/disable <Cisco 1000 Series lightweight access point name> <IP addr> <IP mask> <gateway>

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	static-ip	Cisco 1000 Series lightweight access point static IP address

	[enable/	Configure the Cisco 1000 Series lightweight access point static IP address
	disable]	Disable the Cisco 1000 Series lightweight access point static IP address. The AP will use DHCP to get the IP address.
	<Cisco 1000 Series lightweight access point name>	Cisco 1000 Series lightweight access point name.
	<IP address>	Cisco 1000 Series lightweight access point IP address
	<IP mask>	IP Mask
	<gateway>	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 wlan

To enable or disable WLAN Override for a Cisco 1000 Series lightweight access point radio, and to add or delete WLANs to or from a Cisco 1000 Series lightweight access point radio, as described in the Product Guide, use the config ap wlan commands.

>config ap wlan [add/delete/enable/disable] [802.11a/802.11b] (WLAN ID)
<Cisco 1000 Series lightweight access point>

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	wlan	Reset command.
	enable/disable/	Enable or disable WLAN Override mode.
	add/delete	Add or delete a WLAN override. (Cisco 1000 Series lightweight access point must have WLAN Override enabled to add or delete a WLAN.)
	802.11a/802.11b	802.11a or 802.11b/g radio.
	(WLAN ID)	Optional Cisco Wireless LAN Controller ID assigned to a WLAN.
	<Cisco 1000 Series lightweight access point>	Cisco 1000 Series lightweight access point name.

Defaults (none)

Example **>config ap wlan enable 802.11a AP03**
to enable WLAN Override on the AP03 802.11a radio.

>config ap wlan add 802.11a 1 AP03
to add WLAN ID 1 on the AP03 802.11a radio.

>config ap wlan delete 802.11a AP03
to delete WLAN ID 1 from the AP03 802.11a radio.

>config ap wlan disable 802.11a AP03
to disable WLAN Override on the AP03 802.11a radio.

Related Commands show ap wlan

config exclusionlist

To create or delete an Exclusion List (blacklisted) entry, use the config exclusionlist command.

>config exclusionlist [add/delete] <MAC addr> [description]

Syntax	config exclusionlist	Configure the Exclusion List.
	add/delete	Creates/deletes a local Excluded entry.
	MAC addr	MAC address of the local Excluded entry.
	description	Sets the description for a 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 the Cisco Wireless LAN Controller boot option, use the config boot command.

>config boot [primary/backup]

Syntax	config boot	Configure boot option.
	primary/backup	Primary image or backup image.
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	config certificate	Command action.
	generate	Generates new certificates.
	webadmin	Generates a new web administration certificate
	webauth	Generates a new web authentication certificate
	compatibility[on/off]	Enables or disables compatibility mode for inter-switch ipsec
Defaults	N/A	
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 Address>

Syntax	config	Configure parameters.
	client	Network client.
	deauthenticate	Deauthenticate command.
	<MAC address>	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 country code, use the config country command. Use the show country command to display a list of supported countries. Note that the supported country codes are described in the Cisco SWAN Supported Country Codes section in the Product Guide.

>config country <country-code>

Syntax	config	Configure parameters.
	country	Set this Cisco Wireless LAN Controller to comply with selected country's regulations.
	<country-code>	Select country.
Defaults	Country code = US (United States of America).	
Examples	**>config country US** to configure the country code for use in the United States of America, which allows 802.11a and 802.11b/g transmissions.	

Note: The Cisco Wireless LAN Controller Country Code only operates with Cisco 1000 Series lightweight access points designed for operation in the associated Regulatory Domain. Refer to the Cisco SWAN Supported Country Codes in the Product Guide for Cisco Wireless LAN Controller Country Code mapping to Cisco 1000 Series light-weight access point Regulatory Domains.

Related Commands show country

config custom-web

To configure the custom-web authentication page, use the config custom-web command.

>config custom-web {redirectUrl <string>/weblogo [enable/disable]/webmessage <string>/webtitle <string>/ext-webauth-mode [enable/disable]/ext-webauth-url <ExternalAuthorizationURL>}

Syntax	config custom-web	Command action.
	redirectUrl <string>	Enable/disable the custom redirect URL.
	weblogo [enable/disable]	Enable/disable the Web Authentication logo.
	webmessage <string>	Set the customer message text for Web Authentication.
	webtitle <string>	Set the custom title text for Web Authentication.

	ext-webauth-mode	Enable or disable external URL web-based client authorization.
	ext-webauth-url	The URL used for web-based client authorization.

Defaults (none)

Examples
```
>config custom-web redirectUrl abc.com
>config custom-web weblogo/weblogo enable
>config custom-web webmessage Thisistheplace
>config custom-web webtitle Helpdesk
>config custom-web ext-webauth-mode enable
>config custom-web ext-webauth-url http://www.AuthorizationURL.com/
```

Related Commands show custom-web

config dhcp

To configure the DHCP, use the config dhcp command. Use the show dhcp command to display dhcp configuration.

```
>config dhcp
```

Syntax

config dhcp	Command action.
address-pool <scope name> <start> <end>	Configure an address range to allocate.
create-scope <name>	Create a new dhcp scope.
default-router <scope>	Configure the default routers.
delete-scope <scope name>	Delete a dhcp scope.
disable <enable/disable> <scope name>	Disable a scope.
dns-servers <scope name> <dns1> [dns2] [dns3]	Configure the name servers.
domain <scope name> <domain>	Configure the DNS Domain Name.
enable <enable/disable> <scope name>	Enable a scope
lease <scope name> <lease seconds>	Configure the lease time (in seconds).
netbios-name-server <scope name> <wubs1> [wins2] [wins2] [wins3]	Configure the netbios name servers.
network <scope name> <network> <netmask>	Configure the network and netmask.

Defaults None.

Examples **>config dhcp lease 003**
Configures the dhcp lease for the scope 003

Related Commands show dhcp

config known ap

To configure a known AP, use the config known ap command. T

```
>config known ap <add/alert/delete> <Known AP MAC address>
```

Syntax	config	Configure parameters.
	known ap	Known access point.
	add/alert/delete	Command action.
	<MAC address>	MAC address of the known AP.

Defaults (none)

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

Related Commands config ap

CONFIG INTERFACE COMMANDS

Use the following config interface commands:

- *config interface acl*
- *config interface address*
- *config interface create*
- *config interface delete*
- *config interface dhcp*
- *config interface hostname*
- *config interface port*
- *config interface vlan*

config interface acl

To configure an interface's Access Control List, use the config interface acl command.

>config interface acl <ap-manager/management/vlan-intf-name> <ACL name/none>

Syntax	config interface acl	Command action
	ap-manager	Configures the AP Manager interface.
	management	Configures the management interface.
	<vlan-intf-name>	Enter interface name.
	<ACL name/none>	Access control list or none.

Defaults N/A

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 <ipaddress>/management <addr> <netmask> <gateway>/service port <addr> <netmask>/virtual <addr>] <interface-name>

Syntax	config interface address	Command action.
	ap-manager <IP address>	Configures the AP Manager interface.
	management <addr> <netmask> <gateway>	Configures the management interface.
	service-port <addr>	Configures the out-of-band service Port.

	<netmask>	
	virtual <addr>	Configures the virtual gateway interface.
	<interface-name>	Enter interface name.

Defaults N/A

Examples **>config interface address ap-manger 172.168.2.3**

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	config interface create	Command action
	<interface-name>	Interface name.
	<vlan-id>	VLAN id.

Defaults N/A

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	config interface delete	Command action.
	<interface-name>	Interface name.

Defaults N/A

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/management/service-port <interface-name>

Syntax	config interface dhcp	Command action.
	ap-manager	Configures the AP Manager interface.
	management	Configures the Management Interface.
	service-port	Configures the out-of-band service Port with disable or enable.
	<interface-name>	Enter interface name.

Defaults N/A

Examples **>config interface dhcp service-port DHCP02**

Related Commands show interface

config interface hostname

To configure the virtual interface's virtual DNS host name, use the config interface hostname command.

>config interface hostname <virtual> <DNS Host Name>

Syntax	config interface hostname	Command action.
	virtual	Configures the virtual gateway interface. (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.)
	<DNS Host Name>	DNS Host Name.
Defaults	N/A	
Examples	**>config interface hostname 1.1.1.1 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/vlan-intf-name> <port number>

Syntax	config interface port	Command action.
	ap-manager	AP management interface
	management	The Management Interface.
	vlan-intf-name	VLAN or interface name
	<port number>	Port number for the interface.
Defaults	N/A	
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 <management/vlan-intf-name> <vlan>

Syntax	config interface vlan	Command action.
	management	The management interface.
	vlan-intf-name	VLAN identifier name.
	<vlan>	VLAN id.
Defaults	N/A	
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 <client count>

Syntax	config	Configure parameters.
	load-balancing	Aggressive load-balancing
	status[enable/disable]	Enable or disable the aggressive load balancing status
	window<client count>	Set the aggressive load balancing client window with the number of clients from 0 to 20.
Defaults	Enabled	
Examples	**>config load-balancing enable**	
Related Command	show load-balancing	

config loginsession close

To close active telnet sessions, use the config loginsession close command. Use this command to terminate an individual or all active telnet sessions with the Cisco Wireless LAN Controller. If you are using a telnet session for your CLI interface and terminate your session or all sessions, you will need to reconnect and log back into the Cisco Wireless LAN Controller.

>config loginsession close [<session id>/ all]

Syntax	config	Configure parameters.
	loginsession	Telnet sessions.
	close	Terminate session.
	<session id>	Terminate a specific telnet session.
	all	Terminate all telnet sessions.
Defaults	(none)	
Examples	**>config loginsession close all**	
Related Commands	show loginsession	

CONFIG MACFILTER COMMANDS

Use the following config macfilter commands.

- *config macfilter add*
- *config macfilter delete*
- *config macfilter description*
- *config macfilter interface*
- *config macfilter mac-delimiter*
- *config macfilter radius-compat*
- *config macfilter wlan-id*

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 WLAN on the Cisco Wireless LAN Controller. This filter bypasses the RADIUS authentication process.

>config macfilter add <MAC address> <WLAN ID>[interface name][description]

Syntax	config	Configure parameters.
	macfilter	Local MAC address filter.
	add	Add a client.
	<MAC address	Client MAC address.
	<WLAN ID>	Client WLAN.
	[interface name]	Name of the interface
	[description]	Short description of the interface
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.

>config macfilter delete <MAC addr>

Syntax	config	Configure parameters.
	macfilter	Local MAC address filter.
	delete	Delete a client.
	<MAC addr>	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.

>config macfilter description <MAC addr> <username>"<description>"

Syntax	config	Configure parameters.
	macfilter	Local MAC address filter.
	delete	Delete a client.
	<MAC address>	Client MAC address.
	<username>	An existing MAC filter username.
	"<description>"	Optional description, up to 32 characters, in double quotes.
Defaults	(none)	
Examples	**>config macfilter description 11:11:11:11:11:11 engineer1 "MAC Filter 01"**	
Related Commands	show macfilter	

config macfilter interface

Use to add a MAC filter client interface name.

>config macfilter interface <MAC addr> <interface>

Syntax	config	Configure parameters.
	macfilter	Local MAC address filter.
	interface	Interface name.
	<MAC address>	Client MAC address.
	<interface>"	interface 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 (none, colon, or hyphen) for MAC addresses sent to RADIUS servers, use the config macfilter mac-delimiter command.

>config macfilter mac-delimiter <colon|hyphen|none|single-hyphen>

Syntax	config	Configure parameters.
	macfilter	Local MAC address filter.
	mac-delimiter	MAC address format for RADIUS servers.
	<none|colon|hyphen|single-hyphen>	MAC delimiter format. ("none" disables delimiters.)
Defaults	(none)	
Examples	**>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 aa-bb-cc-dd-ee-ff. **>config macfilter mac-delimiter none** To have OS send MAC address to RADIUS servers in the form aabbccddeeff.	
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	config	Configure parameters.
	macfilter	Local MAC address filter.
	radius-compat	Compatibility with selected RADIUS server.
	{cisco/free/other}	RADIUS server compatibility.
Defaults	Other.	
Examples	**>config macfilter radius-compat other**	
Related Commands	show macfilter	

config macfilter wlan-id

To modify a client WLAN, use the config macfilter wlan-id command.

>config macfilter wlan-id <MAC address> <wlan-id>

Syntax	config	Configure parameters.
	macfilter	Local MAC address filter
	wlan-id	Modify client WLAN
	<MAC address	Client MAC address
	<wlan-id>	New WLAN identification number
Defaults	(none)	
Examples	**>config macfilter wlanid 11:11:11:11:11:11 2**	
Related Commands	show macfilter, show wlan	

CONFIG MGMTUSER COMMANDS

Use the following config mgmtuser commands:

- *config mgmtuser add*
- *config mgmtuser delete*
- *config mgmtuser description*
- *config mgmtuser password*

config mgmtuser add

To add a management user login to the Cisco Wireless LAN Controller, use the config mgmtuser add command.

>config mgmtuser add <username> <password> [read-write/ read-only][description]

Syntax	config	Configure parameters.
	mgmtuser	Management user account
	add	Add a management user account
	<username>	Account username
	<password>	Account password
	[read-write/read-only]	Account privileges
	[description]	Short description
Defaults	(none)	
Examples	**>config mgmtuser add admin admin read-write**	
Related Commands	show mgmtuser	

config mgmtuser delete

To delete a management user login to the Cisco Wireless LAN Controller, use the config mgmtuser delete command.

>config mgmtuser delete <username>

Syntax	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	config	Configure parameters.
	mgmtuser	Management user account.
	description	Delete a management user account.
	<username>	Account username.
	<description>	Account description, up 24 alphanumeric characters,.

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	config	Configure parameters.
	mgmtuser	Management user account
	password	Add a management user account
	<username>	Account username up to 24 alphanumeric characters.
	<password>	New password

Defaults (none)

Examples
```
>config mgmtuser password admin
```

Related Commands show mgmtuser

CONFIG MIRROR COMMANDS

Use the following config mirror commands.

- *config mirror ap*
- *config mirror foreignap*
- *config mirror mac*

- *config mirror port*

config mirror ap

To have all Cisco 1000 Series lightweight access point transmit and receive data appear on the Mirror Port (see *config mirror port*) for troubleshooting, use the config mirror ap command.

>config mirror ap [enable/disable] <AP name>

Syntax	config	Configure parameters.
	mirror	Mirror command.
	ap	Cisco 1000 Series lightweight access point.
	[enable/disable]	Enable or Disable Mirroring for this Cisco 1000 Series lightweight access point.
	<AP name>	Cisco 1000 Series lightweight access point name.

Defaults (none)

Examples **>config mirror ap enable AP5**
configures the Cisco Wireless LAN Controller so the Cisco 1000 Series light-weight access point AP5 data stream is Mirrored on the port selected using the *config mirror port* command.

Related Commands config mirror foreignap, config mirror mac, config mirror port, show mirror ap, show mirror foreignap, show mirror mac, show mirror port

config mirror foreignap

To have all transmit and receive data from a Third-Party AP appear on the Mirror Port (see *config mirror port*) for troubleshooting, use the config mirror foreignap command.

>config mirror foreignap [enable/disable] <port number>

Syntax	config	Configure parameters.
	mirror	Mirror command.
	foreignap	Third-Party Access Point.
	[enable/disable]	Enable or Disable Mirroring for this Third-Party AP.
	<port number>	Front-panel port the Third-Party AP is connected to.

Defaults (none)

Examples **>config mirror foreignap enable 3**
configures the Cisco Wireless LAN Controller so the data stream from the Third-Party AP on Port 3 is Mirrored on the port selected using the *config mirror port* command.

Related Commands config mirror ap, config mirror mac, config mirror port, show mirror ap, show mirror foreignap, show mirror mac, show mirror port

config mirror mac

To have all client transmit and receive data appear on the Mirror Port (see *config mirror port*) for troubleshooting, use the config mirror mac command.

>config mirror mac [enable/disable] <MAC Address>

Syntax	config	Configure parameters.
	mirror	Mirror command.

	mac	Cisco 1000 Series lightweight access point.
	[enable/disable]	Enable or Disable Mirroring for this Cisco 1000 Series lightweight access point.
	<MAC address>	Cisco 1000 Series lightweight access point MAC address.

Defaults (none)

Examples **>config mirror mac enable 02:03:sd:66:85:4a**
configures the Cisco Wireless LAN Controller so the data stream from client 02:03:sd:66:85:4a is Mirrored on the port selected using the *config mirror port* command.

Related Commands config mirror ap, config mirror foreignap, config mirror port, show mirror ap, show mirror foreignap, show mirror mac, show mirror port

config mirror port

(Unused command.)

CONFIG MOBILITY COMMANDS

Use the following config mobility commands:

- *config mobility group member*
- *config mobility secure-mode*
- *config mobility statistics*

config mobility group member

To add or delete users from the Controller Mobility Group member list, use the config mobility group member command.

>config mobility group member [add/delete] <MAC address>

Syntax	config	Configure parameters.
	mobility group	Controller Mobility Group member.
	[add/delete]	Enable or disable Controller Mobility Group feature.
	<MAC address>	Client MAC address.

Defaults (none)

Examples **>config mobility group member add 11:11:11:11:11:11**

Related Commands show mobility

config mobility secure-mode

To enable or disable secure mode for the mobility messages between Controller Mobility Group members, use the config mobility secure-mode command.

>config mobility secure-mode [enable/disable]

Syntax	config	Configure parameters.
	mobility	Controller Mobility Group member.
	secure-mode	Secure mode.

	[enable/disable]	Enable or disable Controller Mobility Group message security.

Defaults (none)

Examples **>config mobility secure-mode enable**

Related Commands show mobility summary

config mobility statistics

To reset the Controller Mobility Group statistics, use the config mobility statistics command.

>config mobility statistics reset

Syntax	config	Configure parameters.
	mobility	Controller Mobility Group.
	statistics	Controller Mobility Group statistics.
	reset	Reset the Controller Mobility Group statistics.

Defaults (none)

Examples **>config mobility statistics reset**

Related Commands show mobility statistics
show mirror foreignap, show mirror mac, show mirror port

CONFIG MSGLOG LEVEL COMMANDS

Use the following msglog level commands:

- *config msglog level critical*
- *config msglog level error*
- *config msglog level security*
- *config msglog level warning*
- *config msglog level verbose*

config msglog level critical

To reset the message log so it only collects and displays critical (highest-level) messages, use the config msglog level critical command. Note that the message log always collects and displays critical messages, regardless of the message log level setting.

>config msglog level critical

Syntax	config	Configure parameters.
	msglog level	Message log message 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 it only collects and displays critical (highest-level) and error (second-highest) messages, use the config msglog level error command.

>config msglog level error

Syntax	config	Configure parameters.
	msglog level	Message log message levels.
	error	Collect and display 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 it only 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	config	Configure parameters.
	msglog level	Message log message levels.
	security	Collect and display security messages.

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 it only 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	config	Configure parameters.
	msglog level	Message log message levels.
	warning	Collect and display warning messages.

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 it collects and displays all messages, use the config msglog level verbose command.

>config msglog level verbose

Syntax	config	Configure parameters.
	msglog level	Message log message 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 NETUSER COMMANDS

Use the following config netuser commands.

- *config netuser add*
- *config netuser delete*
- *config netuser description*
- *config netuser maxUserLogin*
- *config netuser password*
- *config netuser wlan-id*

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	config	Configure parameters.
	netuser	Local network user.
	add	Add a user.
	<username>	Network username of up to 24 alphanumeric characters.
	<password>	User password.
	<WLAN ID	WLAN assigned to the user.
	[description]	Short optional description

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	config	Configure parameters.
	netuser	Local network user.
	delete	Add a user.
	<username>	Network username of 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	config	Configure parameters.
	netuser	Local network user of up to 24 alphanumeric characters.
	description	Add a user description.
	<username>	Network username.
	"<description>"	Net user description, up to 32 alphanumeric characters, in double quotes.
Defaults	(none)	
Examples	**>config netuser description able1 "HQ1 Contact"**	
Related Commands	show netuser	

config netuser maxUserLogin

To set the maximum number of simultaneous users using the same login, use the config netuser maxUserLogin command.

>config netuser maxUserLogin <count>

Syntax	config	Configure parameters.
	netuser	Local network user.
	maxUserLogin	Maximum number of simultaneous users using the same login.
	<count>	Maximum number of logins under the same username (0 to 8).
Defaults	Unlimited (0).	
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	config	Configure parameters.
	netuser	Local network user
	password	Modify the password
	<username>	Network username of up to 24 alphanumeric characters.
	<password>	New user password
Defaults	(none)	
Examples	**>config netuser password aire1 aire2**	
Related Commands	show netuser	

config netuser wlan-id

To change a user WLAN ID, use the config netuser wlan-id command.

>config netuser wlan-id <username> <WAN ID>

Syntax	config	Configure parameters.
	netuser	Local network user
	wlan-id	Modify the WLAN ID
	<username>	Network username of up to 24 alphanumeric characters.
	<WLAN ID	New WLAN assigned to the user
Defaults	(none)	
Examples	**>config netuser wlan-id aire1 2**	
Related Commands	show netuser, show wlan summary	

CONFIG NETWORK COMMANDS

Use the following config network commands:

- *config network ap-fallback*
- *config network apple-talk*
- *config network arptimeout*
- *config network master-base*
- *config network mgmt-via-wireless*
- *config network multicast*
- *config network otap-mode*
- *config network peer-blocking*
- *config network rf-mobility-domain*
- *config network secureweb*
- *config network ssh*

- *config network telnet*
- *config network usertimeout*
- *config network webmode*

config network ap-fallback

To enable or disable AP fallback, use the config network ap-fallback command.

>config network ap-fallback <enable/disable>

Syntax	config	Configure parameters.
	network	Cisco Wireless LAN Controller network parameter.
	ap-fallback	AP fallback.
	<enable/disable>	Enable or disable.
Default	Enabled.	
Examples	>**config network ap-fallback enable**	
Related Commands	show network	

config network apple-talk

To enable or disable apple talk, use the config network apple-talk command.

>config network apple-talk <enable/disable>

Syntax	config	Configure parameters.
	network	Cisco Wireless LAN Controller network parameter.
	apple-talk	Modify Apple-talk
	<enable/disable>	Enable or disable.
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	config	Configure parameters.
	network	Cisco Wireless LAN Controller network parameter.
	arptimeout	Modify the ARP timeout value.
	<seconds>	Timeout in seconds.
Defaults	300 with a minimum of 10.	
Examples	>**config network arptimeout 240**	
Related Commands	show network	

config network master-base

To set the Cisco Wireless LAN Controller as a 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.

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	config	Configure parameters.
	network	Cisco Wireless LAN Controller network parameter.
	master-base	Master Cisco Wireless LAN Controller.
	<enable/disable>	Enables or disables a Cisco Wireless LAN Controller acting as an AP default master.

Defaults (none)

Examples **>config network master-base**

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 that this feature allows wireless clients to manage only the Cisco Wireless LAN Controller associated with the client AND the associated Cisco 1000 Series light-weight 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	config	Configure parameters.
	network	Cisco Wireless LAN Controller network parameter.
	mgmt-via-wireless	Management sessions.
	[enable/disable]	Enable or disable.

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 feature, use the config network multicast command.

>config network multicast [enable/disable]

Syntax	config	Configure parameters.
	network	Network parameters.
	multicast	Ethernet multicast mode.
	[enable/disable]	Change the multicast state.

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	config	Configure parameters.
	network	Network parameters.
	otap-mode	Over-the-air Cisco 1000 Series lightweight access point provisioning.
	[enable/disable]	Change the OTAP state.

Defaults Enabled.

Examples >**config network otap-mode disable**

Related Commands show network

config network peer-blocking

Disabled allows same-subnet clients to communicate through the Cisco Wireless LAN Controller. Enabled (default) forces same-subnet clients to communicate through a higher-level router. To enable or disable peer blocking, use the config network peer-blocking command.

>config network peer-blocking [enable/disable]

Syntax	config	Configure parameters.
	network	Network parameters.
	peer-blocking	Peer communications requirement.
	[enable/disable]	Change the peer-blocking state.

Defaults Disabled.

Examples >**config network peer-blocking enable**

Related Commands show network

config network rf-mobility-domain

To set the RF Controller Mobility Group domain name, use the config network rf-mobility-domain command.

>config network rf-mobility-domain <domain_name>

Syntax	config	Configure parameters.
	network	Cisco Wireless LAN Controller network parameter.
	rf-mobility-domain	Controller Mobility Group domain.
	<domain_name>	Controller Mobility Group name, an ASCII string of up to 31 characters (case-sensitive).

Defaults (none)

Examples >**config network rf-mobility-domain travelers_group**

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	config	Configure parameters.
	network	Network parameters.
	secureweb	Secure Web User Interface.
	[enable/disable]	Change the interface state.
Defaults	Enabled.	
Examples	>**config network secureweb enable**	
Related Commands	show network	

config network ssh

To change the state of Secure Shell sessions, use the config network ssh command.

>config network ssh [enable/disable]

Syntax	config	Configure parameters.
	network	Network parameters.
	ssh	Secure Shell sessions
	[enable/disable]	Change the state of the SSH session.
Defaults	Enabled.	
Examples	>**config network ssh enable**	
Related Commands	show network	

config network telnet

To change the state of telnet sessions, use the config network telnet command.

>config network telnet [enable/disable]

Syntax	config	Configure parameters.
	network	Network parameters.
	telnet	Telnet sessions.
	[enable/disable]	Change the state of the telnet session.
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	config	Configure parameters.
	network	Network parameters.
	usertimeout	Timeout for sessions.
	<seconds>	Duration in seconds.
Defaults	300, minimum is 10.	
Examples	**>config network usertimeout 1200**	
Related Commands	show network	

config network webmode

To enable or disable web access, use the config network webmode command.

>config network webmode [enable/disable]

Syntax	config	Configure parameters.
	network	Network parameters.
	webmode	Web User Interface.
	[enable/disable]	Change the interface state.
Defaults	Enabled.	
Examples	**>config network webmode disable**	
Related Commands	show network	

CONFIG PORT COMMANDS

Use the following config port commands:

- *config port adminmode*
- *config port autoneg*
- *config port linktrap*
- *config port multicast*
- *config port physicalmode*
- *config port power*

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 [<port>/all] [enable/disable]

Syntax	config	Configure parameters.
	port	Port parameters
	adminmode	Administrative mode
	[<port>/all]	Individual port number or all ports
	[enable/disable]	Port state
Default	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 that 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 [<port>/all] [enable/disable]

Syntax		
	config	Configure parameters.
	port	10/100BASE-T Ethernet.
	<port>	Physical port number.
	all	All Ports.
	enable	Turn autonegotiation on.
	disable	Turn autonegotiation off.

Defaults All Ports = autonegotiation enabled.

Examples **>config port autoneg all enable**
to turn on physical port autonegotiation for all front-panel Ethernet ports.

>config port autoneg 19 disable
to disable physical port autonegotiation for front-panel Ethernet port 19.

Related Commands show port, config port physicalmode

config port linktrap

To change 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 [<port>/all] [enable/disable]

Syntax		
	config	Configure parameters.
	port	Port parameters.
	linktrap	Link status alert.
	[<port>/all]	Individual port number or all ports.
	[enable/disable]	Port state.

Default 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 vlan [<port>/all] [enable/disable]

Syntax	config	Configure parameters.
	port	Port parameters.
	multicast	Multicast appliance.
	vlan	Vlan
	[<port>/all]	Individual port number or all ports.
	[enable/disable]	Port state.
Default	Enabled.	
Example	To enable all port traps: **>config port multicast vlan all 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 [<port>/all] [enable/disable] [100h/100f/10h/10f]

Syntax	config	Configure parameters.
	port	Port parameters.
	physicalmode	Port physical mode.
	[<port>/all]	Individual port number or all ports
	[enable/disable]	Port state
	[100h/100f/10h/10f]	o 100h = 100 Mbps/Half Duplex operation o 100f = 100 Mbps/Full Duplex operation o 10h = 10 Mbps/Half Duplex operation o 10f = 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 change Power over Ethernet (PoE) settings for a single port or all Cisco Wireless LAN Controller ports, use the config port power command. NOT ALL APs are PoE (802.3af) compatible! If you are using Third-Party access points, refer to your user documentation to determine compatibility. Enabling PoE to non-compatible APs can result in severe equipment damage including fire!

>config port power [<port>/all] [enable/disable]

Syntax	config	Configure parameters.
	port	Port parameters
	power	PoE mode
	[<port>/all]	Individual port number or all ports
	[enable/disable]	Port state
Default	Enabled	
Examples	To disable PoE on port 8: **>config port power 8 disable**	
	To enable PoE on all ports: **>config port power all enable**	
Related Commands	show port	

config prompt

To change the CLI system prompt, use the config prompt command.

This command can be used any time the CLI interface is active.

>config prompt <system prompt>

Because the system prompt is a user-defined variable, it is omitted from the rest of this documentation.

Syntax	config	Configure parameters.
	prompt	CLI system prompt, up to 31 alphanumeric characters.
	<system prompt>	New CLI system prompt, in double quotes.
Defaults	The system prompt is configured using the startup wizard.	
Examples	(old CLI prompt >**config prompt "Type here"** Type here>	
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	config qos	Command action.
	queue_length	Configure QoS queue length.
	bronze/silver/gold/	Level of quality of service: Background, Best Effort,
	<length>	Queue length.
Defaults	N/A	

Examples **>config qos queue_length gold 12**

Related Commands show qos queue_length all

CONFIG RADIUS ACCT COMMANDS

Use the following config radius acct commands:

- *config radius acct add*
- *config radius acct delete*
- *config radius acct disable*
- *config radius acct enable*

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 addr> <port> <ascii/hex> <secret>

Syntax	config	Configure parameters.
	radius acct	RADIUS accounting server.
	add	Add a RADIUS server.
	<index>	Priority index (Cisco Wireless LAN Controller begins search with 1).
	<IP addr>	IP Address.
	<port>	Port number for the interface protocols.
	<ascii/hex>	ASCII or Hex
	<secret>	Login password.

Defaults When added the port number defaults to 1813 and state is enabled.

Examples **>config radius acct add 1 10.10.10.10 1813 ascii admin**
to configure a priority 1 RADIUS server at 10.10.10.10 using port 1813 with a login password of 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 add <index>

Syntax	config	Configure parameters.
	radius acct	RADIUS accounting server.
	delete	Remove a RADIUS server.
	<index>	Priority 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	config	Configure parameters.
	radius acct	RADIUS accounting server.
	disable	Disable a RADIUS server.
	<index>	Priority 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	config	Configure parameters.
	radius acct	RADIUS accounting server.
	enable	Enable a RADIUS server.
	<index>	Priority index.
Defaults	(none)	
Examples	>**config radius acct enable 1**	
Related Commands	show radius acct statistics	

CONFIG RADIUS AUTH COMMANDS

Use the following config radius auth commands:

- *config radius auth add*
- *config radius auth delete*
- *config radius auth disable*
- *config radius auth enable*

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 addr> <port> <ascii/hex> <secret>

Syntax	config	Configure parameters.
	radius auth	RADIUS authentication server.
	add	Add a RADIUS server.
	<index>	Priority index (Cisco Wireless LAN Controller begins search with 1).

	<IP addr>	IP Address.
	<port>	Port number for the interface protocols.
	<ascii/hex>	ASCII or Hex.
	<secret>	Login password.

Defaults When added the port number defaults to 1812 and state is enabled.

Examples **>config radius auth add 1 10.10.10.10 1812 ascii admin**
to configure a priority 1 RADIUS server at 10.10.10.10 using port 1812 with a login password of 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 add <index>

Syntax	config	Configure parameters.
	radius auth	RADIUS authentication server.
	delete	Remove a RADIUS server.
	<index>	Priority 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	config	Configure parameters.
	radius auth	RADIUS authentication server.
	disable	Disable a RADIUS server.
	<index>	Priority 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 acct enable <index>

Syntax	config	Configure parameters.
	radius auth	RADIUS authentication server.

	enable	Enable a RADIUS server.
	<index>	Priority index.

Defaults (none)

Examples >**config radius auth enable 1**

Related Commands show radius auth statistics

config radius backward compatibility

To enable RADIUS backward compatibility for the Cisco Wireless LAN Controller, use the config radius backward command.

>config radius backward compatibility [enable/disable]

Syntax	config	Configure parameters.
	radius backward compatibility	RADIUS authentication server.
	[enable/disable]	Backward compatibility state.

Defaults Enabled.

Examples >**config radius backward compatibility disable**

Related Commands show radius summary

config radius callStationIdType

To enable callStationIdType for the Cisco Wireless LAN Controller, use the config radius callStationId-Type 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	config	Configure parameters.
	callStationIdType	
	ipAddr	Cisco Wireless LAN Controller IP address.
	macAddr	Cisco Wireless LAN Controller MAC address.
	ap-macAddr	Cisco 1000 Series lightweight access point MAC address.

Defaults Enabled.

Examples >**config radius callStationIdType ipAddr** (Layer 3 Only)
>**config radius callStationIdType macAddr** (Layers 2 and/or 3)
>**config radius callStationIdType ap-macAddr** (Layers 2 and/or 3)

Related Commands show radius summary

config rogue ap

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

>config rogue ap <acknowledged/alarm/known> <MAC address> <num of APs>

Syntax	config	Configure parameters.
	rogue ap	Rogue AP status.

	acknowledged	This AP has been identified and belongs to an external network.
	alarm	This AP has not been identified. Generates a trap upon detection of this access point.
	known	This AP has been identified and is part of an internal network.
	<MAC address>	MAC address of the AP.
	<num of APs>	Number of APs.

Defaults (none)

Example **>config rogue ap acknowledge 11:11:11:11:11:11**

Related Commands show rogue ap summary, show rogue ap detailed, config rogue ap

config rogue adhoc

To configure the status of an adhoc rogue access point (IBSS), use the config rogue adhoc command.

>config rogue adhoc <acknowledged/alarm/known/contain> <MAC address> <num of APs>

Syntax	config	Configure parameters.
	rogue adhoc	Adhoc Rogue AP.
	acknowledged	This AP has been identified and belongs to an external network.
	alarm	This AP has not been identified. Generates a trap upon detection of this access point.
	known	Information known about this AP
	contain	Start containing an adhoc rogue access point.
	<MAC address>	MAC address of the adhoc rogue.
	<num of APs>	Number of APs.

Defaults (none)

Example **>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 address> <num of APs>

Syntax	config	Configure parameters.
	rogue client	Rogue client status.
	alert	This client has not been identified. Generates a trap upon detection of this access point.
	contain	Start containing a rogue access point.
	<MAC address>	MAC address of the AP.
	<num of APs>	Number of APs.

Defaults (none)

Example **>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 following config route commands:

- *config route add*
- *config route delete*

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 <Network IP address> <IP netmask> <gateway>

Syntax	config	Configure parameters.
	route	Network route.
	add	Add a route.
	<Network IP Address>	Destination network IP Address range.
	<IP netmask>	Destination subnet mask.
	<gateway>	IP Address of the Service Port gateway router.
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 <Network IP address>

Syntax	config	Configure parameters.
	route	Network route.
	delete	Delete a route.
	<Network IP Address>	Destination network IP Address range.
Defaults	(none)	
Examples	>**config route delete 10.1.1.0**	
Related Commands	show route all, config route add	

CONFIG SERIAL COMMANDS

Use the following config serial commands:

- *config serial baudrate*
- *config serial timeout*

config serial baudrate

To set the serial baud rate, use the config serial baudrate command.

>config serial [1200/2400/4800/9600/19200/38400/57600/115200]

Syntax	config	Configure parameters.

	serial	Serial connection settings.
	[1200/2400/4800/9600/ 19200/38400/57600/ 115200]	Connection speed.

Defaults 9600.

Examples **>config serial baudrate 9600**

Related Commands config serial timeout

config serial timeout

To set the timeout of a serial 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	config	Configure parameters.
	serial	Serial connection settings.
	timeout	Connection duration.
	<minutes>	Timeout in minutes from 0 to 160.

Defaults 0 (no timeout).

Examples **>config serial timeout 10**

Related Commands config serial timeout

CONFIG SESSIONS COMMANDS

Use the following config sessions commands:

- *config sessions maxsessions*
- *config sessions timeout*

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 <0-5>

Syntax	config	Configure parameters.
	sessions	Telnet CLI session parameters.
	maxsessions	Number of allowed CLI sessions.
	<0-5>	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 <0-160>
```

Syntax	config	Configure parameters.
	sessions	Telnet CLI session parameters.
	timeout	Duration of CLI sessions.
	<0-160>	Timeout of telnet session in minutes.
Defaults	5.	
Examples	**>config sessions timeout 20**	
Related Commands	show sessions	

CONFIG SNMP COMMUNITY COMMANDS

Use the following config snmp community commands:

- *config snmp community accessmode*
- *config snmp community create*
- *config snmp community delete*
- *config snmp community ipaddr*
- *config snmp community mode*

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	config	Configure parameters.
	snmp	SNMP parameters.
	community	SNMP community parameters.
	accessmode	Access privileges.
	ro/rw	Read only or Read/Write.
	<name>	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:

```
name    0.0.0.0    0.0.0.0    Read Only   Disable
```

>config snmp community create <name>

Syntax	config	Configure parameters.
	snmp	SNMP parameters.
	community	SNMP community parameters.
	create	Create a new community.
	<name>	Community name of up to 16 characters.
Defaults	(none)	
Examples	>**config snmp community create test**	
Related Commands	show snmp community, config snmp community mode, config snmp community accessmode, config snmp community delete, config snmp community ipaddr	

config snmp community delete

To delete an SNMP community, use the config snmp community delete command.

>config snmp community delete <name>

Syntax	config	Configure parameters.
	snmp	SNMP parameters.
	community	SNMP community parameters.
	delete	Delete a new community.
	<name>	Community name.
Defaults	N/A	
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 modify the IP Address of an SNMP community, use the config snmp community ipaddr command.

>config snmp community ipaddr <ipaddr> <ipmask> <name>

Syntax	config	Configure parameters.
	snmp	SNMP parameters.
	community	SNMP community parameters.
	ipaddr	Set IP Address parameters.
	<ipaddr>	IP Address.
	<ipmask>	Subnet mask.
	<name>	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	config snmp community	Configure SNMP community parameters.
	mode	Change the state.
	<enable/disable>	Enable or disable the community.
	<name>	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	config	Configure parameters.
	snmp	SNMP parameters.
	syscontact	System contact.
	<contact>	Name (Up to 31 alphanumeric characters).
Defaults	(none)	
Examples	**>config snmp syscontact Cisco SWAN_administrator**	
Related Commands	show snmpcommunity	

config snmp syslocation

To set the SNMP system location name, use the config snmp syslocation command.

>config snmp syslocation <location>

Syntax	config	Configure parameters.
	snmp	SNMP parameters.
	syslocation	System location.
	<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 following config snmp trapreceiver commands:

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

- *config snmp trapreceiver mode*

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> <ipaddr>

Syntax	config	Configure parameters.
	snmp	SNMP parameters.
	trapreceiver	SNMP trap server parameters.
	create	Create a new server.
	<name>	Server name.
	<ipaddr>	Server 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	config	Configure parameters.
	snmp	SNMP parameters.
	trapreceiver	Server to receive traps.
	delete	Remove a server.
	<name>	Server name
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	config	Configure parameters.
	snmp	SNMP parameters.
	trapreceiver	Server to receive traps.
	mode	Change the state.
	<enable/disable>	Enable or disable.
	<name>	Server name.
Defaults	(none)	
Examples	**>config snmp trapreceiver mode disable server1**	

Related Commands show snmp trap

CONFIG SNMP V3USER COMMANDS

Use the following config snmp v3user commands:

- *config snmp v3user create*
- *config snmp v3user delete*

config snmp v3user create

To add a version 3 SNMP user, use the config snmp v3user create command.

>config snmp v3user <username> [rw/ro] [none/hmacmd5/hmacsha] [none/des] <authkey> <encrypkey>

Syntax

config	Configure parameters.
snmp	SNMP parameters.
v3user	Version 3 SNMP.
<username>	New username.
[rw/ro]	Read/write or read/only user privileges.
[none/hmacmd5/hmacsha]	Authentication protocol.
[none/des]	Encryption protocol.
<authkey>	Authentication key, if enabled.
<encrypkey>	Encryption key, if enabled.

Defaults

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

Examples **>config snmp v3user test ro 3**
to add an SNMP username test with read-only privileges and no encryption or authentication.

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

config	Configure parameters.
snmp	SNMP parameters.
v3user	Version 3 SNMP.
delete	Remove user.
<username>	Username to delete.

Defaults

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

Examples **>config snmp v3user delete test**
This will remove an SNMP user named 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	config	Configure parameters.
	snmp	SNMP parameters.
	version	Duration of CLI sessions.
	<v1/v2/v3>	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 following config spanningtree port commands:

- *config spanningtree port mode*
- *config spanningtree port pathcost*
- *config spanningtree port priority*

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 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	config	Configure parameters.
	spanningtree	Spanning Tree Protocol.
	port	Cisco Wireless LAN Controller Ethernet port.
	mode	STP mode.
	[off/802.1d/fast]	STP off/802.1D/fast.
	[<port>/all]	Port 1 through 12 or 1 through 24, or all ports.

Defaults Port STP = off.

Examples **>config spanningtree port mode off all**
to disable STP for all Ethernet ports.

>config spanningtree port mode 802.1d 24
to turn on STP 802.1D mode for Ethernet port 24.

>config spanningtree port mode fast 2
to turn on fast STP mode for Ethernet port 2.

Related Commands show spanningtree port, config spanningtree switch mode, config spanningtree port pathcost, config spanningtree port priority

config spanningtree port pathcost

To set the STP path cost for an Ethernet port, use the config spanningtree port pathcost command.

```
>config spanningtree port pathcost [1-65535/auto] [<port>/all]
```

Syntax		
	config	Configure parameters.
	spanningtree	Spanning Tree Protocol.
	port	Cisco Wireless LAN Controller Ethernet port.
	pathcost	STP path cost.
	[1-65535/auto]	Port pathcost, as determined by the network planner, or auto (default)
	[<port>/all]	Port 1 through 12 or 1 through 24, or all ports.

Defaults Pathcost = Automatic.

Examples **>config spanningtree port pathcost auto all**
to have the STP algorithm automatically assign a path cost for all ports.

>config spanningtree port pathcost 200 22
to have the STP algorithm use a port cost of 200 for port 22.

Related Commands show spanningtree port, config spanningtree port mode, config spanningtree port priority

config spanningtree port priority

To configure the STP port priority, use the >config spanningtree port priority command.

```
>config spanningtree port priority [0-255] <port>
```

Syntax		
	config	Configure parameters.
	spanningtree	Spanning Tree Protocol.
	port	Cisco Wireless LAN Controller Ethernet port.
	priority [0-255]	STP priority, 0 through 255.
	<port>	Port 1 through 12 or 1 through 24.

Defaults STP Priority = 128.

Examples **>config spanningtree port priority 100 2**
to set Ethernet port 2 to STP priority 100.

Related Commands show spanningtree port, config spanningtree switch mode, config spanningtree port mode, config spanningtree port pathcost

CONFIG SPANNINGTREE SWITCH COMMANDS

Use the following config spanningtree switch commands:

- *config spanningtree switch bridgepriority*
- *config spanningtree switch forwarddelay*
- *config spanningtree switch hellotime*
- *config spanningtree switch maxage*

- *config spanningtree switch mode*

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.

>config spanningtree switch bridgepriority [0-65535]

Syntax	config	Configure parameters.
	spanningtree	Spanning Tree Protocol.
	switch	Cisco Wireless LAN Controller.
	bridgepriority	Bridge ID.
	[0-65535]	Decimal number range.

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 [4-30]

Syntax	config	Configure parameters.
	spanningtree	Spanning Tree Protocol.
	switch	Cisco Wireless LAN Controller.
	forwarddelay	Forward delay setting.
	[4-30]	Range in seconds.

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 [1 -10]

Syntax	config	Configure parameters.
	spanningtree	Spanning Tree Protocol.
	switch	Cisco Wireless LAN Controller.
	hellotime	Hello time setting.
	[1-10]	Range 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 [6-40]

Syntax	config	Configure parameters.
	spanningtree	Spanning Tree Protocol.
	switch	Cisco Wireless LAN Controller.
	maxage	Forward delay setting.
	[6-40]	Range 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 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	config	Configure parameters.
	spanningtree	Spanning Tree Protocol.
	switch	Cisco Wireless LAN Controller.
	mode	STP mode.
	[enable/disable]	Turn on/off.

Defaults STP = Disabled.

Examples **>config spanningtree switch mode enable**
to support STP on all Cisco Wireless LAN Controller Ports.

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 following config switchconfig commands:

- *config switchconfig flowcontrol*
- *config switchconfig mode*

config switchconfig flowcontrol

To enable or disable 802.3x flow control, use the config switchconfig flowcontrol command.

>config switchconfig flowcontrol [enable/disable]

Syntax	config	Configure parameters.
	switchconfig	Cisco Wireless LAN Controller parameters.
	flowcontrol	Flow control.
	[enable/disable]	Turn on/off.

Defaults Disabled

Examples **>config switchconfig flowcontrol enable**

Related Commands show switchconfig

config switchconfig mode

To configure LWAPP transport mode for Layer 2 or Layer 3, use the config switchconfig flowcontrol command.

>config switchconfig mode [L2/L3]

Syntax	config	Configure parameters.
	switchconfig	Cisco Wireless LAN Controller parameters.
	mode [L2/L3]	Layer 2 or Layer 3 mode.

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 [<ipaddr>/disable]

Syntax	config	Configure parameters.
	syslog	System logs.
	<ipaddr>	Specify an IP Address to send logs.
	disable	Disable 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

config	Configure parameters.
sysname	Cisco Wireless LAN Controller name.
<name>	Name (Up to 31 alphanumeric characters).

Defaults (none)

Examples
```
>config sysname Ent_01
```

Related Commands show sysinfo

config time

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

```
>config time
```

Syntax

config	Command action.
manual MM/DD/YYYY HH:MM:SS	Configures the system time.
ntp Interval/server	Configures the Network Time Protocol Polling Interval or the Network Time Protocol Servers.
timezone <disable/enable> <hours> [minutes]	Disables or enables daylight savings time for the system.

Defaults (none)

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

Related Commands show time

CONFIG TRAPFLAGS COMMANDS

Use the following config trapflags commands:

- *config trapflags 802.11-Security*
- *config trapflags aaa*
- *config trapflags ap*
- *config trapflags authentication*
- *config trapflags client*

- *config trapflags configsave*
- *config trapflags ipsec*
- *config trapflags linkmode*
- *config trapflags multiusers*
- *config trapflags rogueap*
- *config trapflags rrm-params*
- *config trapflags rrm-profile*
- *config trapflags stpmode*
- *config trapflags wps*

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	config	Configure parameters.
	trapflags	Trap parameters.
	802.11-Security	802.11 security traps flag.
	<wepDecryptError>	WEP decryption error.
	[enable/disable]	Modify the state of the parameter.
Defaults	Enabled	
Examples	**>config trapflags aaa disable**	
Related Commands	show trapflags	

config trapflags aaa

To enable or disable sending AAA server related traps, use the config trapflags aaa command.

>config trapflags aaa <auth/servers> [enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	aaa	AAA traps flag.
	<auth/servers>	Authentication/Servers
	[enable/disable]	Modify the state of the parameter.
Defaults	Enabled	
Examples	**>config trapflags aaa auth disable**	
Related Commands	show trapflags	

config trapflags ap

To enable or disable sending Cisco 1000 Series lightweight access point related traps, use the config trapflags ap command.

>config trapflags ap <register/interfaceUp>[enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	ap	Cisco 1000 Series lightweight access point traps flag.
	<register/interfaceUp>	Register/Interface Up
	[enable/disable]	Modify the state of the parameter.
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	config	Configure parameters.
	trapflags	Trap parameters.
	authentication	Authentication of SNMP access.
	[enable/disable]	Modify the state of the parameter.
Defaults	Enabled	
Examples	**>config trapflags authentication disable**	
Related Commands	show trapflags	

config trapflags client

To enable or disable sending 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>[enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	client	DOT11 traps flag.
	802.11-disassocate/ 802.11-deauthenticate/ 802.11-authfail/ 802.11-assocfail>	Enable or send the indicated trap for clients.
	[enable/disable]	Modify the state of the parameter.
Defaults	Disabled	
Examples	**>config trapflags client 802.11-disassociate disable**	
Related Commands	show trapflags	

config trapflags configsave

To enable or disable sending configuration saved trap, use the config trapflags configsave command.

>config trapflags configsave [enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	configsave	Saved configuration trap flag.
	[enable/disable]	Modify the state of the parameter.

Defaults Enabled

Examples **>config trapflags configsave disable**

Related Commands show trapflags

config trapflags ipsec

To enable or disable sending 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	config	Configure parameters.
	trapflags	Trap parameters.
	ipsec	IPSec trap flags.
	<esp-auth/ esp-reply/ nvalidSPI/ ike-neg/suite-neg/ invalid-cookie>	Send IPSec traps when the indicated trap occurs.
	[enable/disable]	Modify the state of the parameter.

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 flag, use the config trapflags linkmode command.

>config trapflags linkmode [enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	linkmode	Link status flag.
	[enable/disable]	Modify the state of the parameter.

Defaults Enabled

Examples **>config trapflags linkmode disable**

Related Commands show trapflags

config trapflags multiusers

To enable or disable sending traps when multiple logins active, use the config trapflags multiusers command.

>config trapflags multiusers [enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	multiusers	Multiple user flag.
	[enable/disable]	Modify the state of the parameter.
Defaults	Enabled	
Examples	**>config trapflags multiusers disable**	
Related Commands	show trapflags	

config trapflags rogueap

To enable or disable sending Rogue AP detection traps, use the config trapflags rogueap command.

>config trapflags rogueap [enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	rogueap	Rogue AP detection trap flag.
	[enable/disable]	Modify the state of the parameter.
Defaults	Enabled	
Examples	**>config trapflags rogueap disable**	
Related Commands	show trapflags	

config trapflags rrm-params

To enable or disable sending RRM profile related traps, use the config trapflags rrm-params command.

>config trapflags rrm-params <tx-power/channel/antenna> [enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	rrm-params	RRM parameters traps flag.
	<tx-power/	Enable sending trap when RF manager automatically changes tx-power level for the Cisco 1000 Series lightweight access point interface.
	channel/	Enable sending trap when RF manager automatically changes channel for the Cisco 1000 Series light-weight access point interface.
	antenna>	Enable sending trap when RF manager automatically changes antenna for the Cisco 1000 Series light-weight access point interface.
	[enable/disable]	Modify the state of the parameter.
Defaults	Enabled	
Examples	**>config trapflags rrm-params tx-power disable**	
Related Commands	show trapflags	

config trapflags rrm-profile

To enable or disable sending RRM profile related traps, use the config trapflags rrm-profile command.

>config trapflags rrm-profile <load/noise/interference/coverage> [enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	rrm-profile	RRM profile traps flag.
	<load/noise/ interference/coverage>	Profile parameters
	[enable/disable]	Modify the state of the parameter.

Defaults Enabled

Examples **>config trapflags rrm-profile load disable**

Related Commands show trapflags

config trapflags stpmode

To enable or disable sending spanning tree traps, use the config trapflags stpmode command.

>config trapflags stpmode [enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	stpmode	Spanning traps flag.
	[enable/disable]	Modify the state of the parameter.

Defaults Enabled

Examples **>config trapflags stpmode disable**

Related Commands show trapflags

config trapflags wps

To enable or disable sending wireless protection system (WPS) traps, use the config trapflags wps command.

>config trapflags wps [enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	wps	Wireless Protection System traps.
	[enable/disable]	Modify the state of the parameter.

Defaults Enabled

Examples **>config trapflags wps disable**

Related Commands show trapflags

CONFIG WATCHLIST COMMANDS

Use the following config watchlist commands.

- *config watchlist add*
- *config watchlist delete*

- *config watchlist enable/disable*

config watchlist add

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

>config watchlist add [mac <MAC addr>/username <Username>]

Syntax	config watchlist	Command action.
	add	Add a watchlist entry.
	mac <MAC addr>	MAC address of new entry.
	username <Username>	Username.
Defaults	(none)	
Examples	**>config watchlist add a5:6b:ac:10:01:6b Able1**	
Related Commands	config watchlist delete, config watchlist enable/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 addr>/username <Username>]

Syntax	config watchlist	Command action.
	delete	Delete a watchlist entry.
	mac <MAC addr>	MAC address of new entry.
	username <Username>	Username.
Defaults	(none)	
Examples	**>config watchlist delete a5:6b:ac:10:01:6b Able1**	
Related Commands	config watchlist add, config watchlist enable/disable, show watchlist	

config watchlist enable/disable

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

>config watchlist enable/disable

Syntax	config watchlist	Command action.
	enable/disable	Enable or disable the client watchlist.
Defaults	(none)	
Examples	**>config watchlist enable** **>config watchlist disable**	
Related Commands	config watchlist add, config watchlist delete, show watchlist	

CONFIG WLAN COMMANDS

- *config wlan aaa-override*
- *config wlan broadcast-ssid*
- *config wlan create*

- *config wlan delete*
- *config wlan dhcp_server*
- *config wlan disable*
- *config wlan enable*
- *config wlan exclusionlist*
- *config wlan interface*
- *config wlan mac-filtering*
- *config wlan qos*
- *config wlan radio*
- *config wlan security*
- *config wlan timeout*
- *config wlan vlan*
- *config wlan wme*

config wlan aaa-override

To create 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 WLAN 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 SWAN WLAN VLAN to a VLAN returned by the AAA server and predefined in the Cisco Wireless LAN Controller Interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the Operating System will also use QoS and ACL provided by the AAA server, as long as they are predefined in the Cisco Wireless LAN Controller Interface configuration. (This VLAN switching by AAA Override is also referred to as Identity Networking.)

For instance, if the Corporate WLAN 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 WLAN 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	config	Configure parameters.
	wlan	Wireless LAN parameters.
	aaa-override	WLAN AAA Override.
	enable/disable	Change state command.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
Defaults	Disabled.	
Examples	>**config wlan aaa-override enable**	
Related Commands	show wlan	

config wlan broadcast-ssid

To configure an SSID broadcast on a WLAN, use the config wlan broadcast-ssid command.

>config wlan broadcast-ssid [enable/disable] <WLAN id>

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	broadcast-ssid	Broadcast SSID.
	enable/disable	Change state command.
	<WLAN id>	WLAN identifier between 1 and 16.
Defaults	Disabled.	
Examples	>**config wlan broadcast-ssid enable**	
Related Commands	show wlan	

config wlan exclusionlist

To modify the 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] <seconds>

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	exclusionlist	Exclusion List.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
	<seconds>	Timeout in seconds.
Defaults	Not enabled	
Examples	>**config wlan exclusionlist foreignAp 2**	
Related Commands	show exclusionlist	

config wlan create

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

>config wlan create <WLAN id> [<WLAN id/foreignAp]

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	create	Add a WLAN.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
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	config	Configure parameters.
	wlan	Wireless LAN parameters.
	delete	Remove a WLAN.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
Defaults	(none)	
Examples	**>config wlan delete foreignAp**	
Related Commands	show wlan, show wlan summary	

config wlan dhcp_server

To configure the DHCP server for a wireless LAN, use the config wlan dhcp_server command.

>config wlan dhcp_server [<WLAN id>/foreignAp] <ipaddr>

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	dhcp_server	Configure DHCP server.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
	<ipaddr>	IP Address of the DHCP server (this parameter is required).
Defaults	(none)	
Examples	**>config wlan dhcp_server foreignAp 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	config	Configure parameters.
	wlan	Wireless LAN parameters.
	disable	Change state of WLAN.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
Defaults	(none)	
Examples	**>config wlan disable foreignAp**	
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	config	Configure parameters.
	wlan	Wireless LAN parameters.
	enable	Change state of WLAN.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
Defaults	(none)	
Examples	**>config wlan enable foreignAp**	
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	config	Configure parameters.
	wlan	Wireless LAN parameters.
	interface	Change state of WLAN.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
	<interface-name>	Existing interface name.
Defaults	(none)	
Examples	**>config wlan interface foreignAp**	
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	config	Configure parameters.
	wlan	Wireless LAN parameters.
	mac-filtering	MAC filtering feature.
	enable/disable	Change state command.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
Defaults	(none)	
Examples	**>config wlan mac-filtering enable 1**	
Related Commands	show wlan	

config wlan qos

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

>config wlan qos [<WLAN id>/foreignAp] [bronze/silver/gold/platinum]

Syntax	config	Configure parameters.

	wlan	Wireless LAN parameters.
	qos	Quality of service.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
	bronze/silver/gold/ platinum	Grades of service: Background, Best Effort, Video, and Voice, respectively.

Defaults (none)

Examples To set the highest level of service on WLAN 1, use the following command:

```
>config wlan qos 1 gold
```

To set a lower level of service for Third-Party APs, use the following command:

```
>config wlan qos foreignAp bronze
```

Related Commands show wlan

config wlan radio

To the set the Cisco Radio policy on a wireless LAN, use the config wlan radio command. Set the WLAN policy to apply to 802.11a, 802.11g, 802.11b, 802.11a/g, 802.11b/g, or All = 802.11a/b/g Cisco Radios.

```
>config wlan radio <WLAN id> [all/802.11a/802.11bg/802.11g/802.11ag]
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	radio	Cisco Radio policy.
	<WLAN id>	WLAN identifier between 1 and 16.
	802.11a	Only 802.11a supported, when 802.11a is enabled.
	802.11bg	Only 802.11b supported, when 802.11b is enabled and 802.11g support is disabled.
	802.11g	Only 802.11g supported, when 802.11b and 802.11g support are enabled.
	all	Only 802.11a/b supported, when 802.11a and 802.11b are enabled and 802.11g support is disabled.
	802.11bg	Only 802.11b/g supported, when 802.11b and 802.11g support are enabled.
	802.11ag	Only 802.11a/g supported, when 802.11a, 802.11b and 802.11g support are enabled.
	all	802.11a/b/g supported, when 802.11a, 802.11b and 802.11g support are enabled.

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 wme

To configure WME, use the config wlan wme command.

```
>config wlan wme <allow/disable/require> [<WLAN id/foreignAp]
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	wme	Configure WME.
	<allow/	Allows WME on the WLAN.
	disable/	Disables WME on the WLAN.
	require>	Requires WME enabled clients on the WLAN.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
Defaults	(none)	
Examples	**>config wlan wme allow 1 SSID01**	
Related Commands	show trapflags	

CONFIG WLAN SECURITY COMMANDS

- *config wlan security 802.1X*
- *config wlan security cranite*
- *config wlan security fortress*
- *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 l2tp*
- *config wlan security passthru*
- *config wlan security static-wep-key*
- *config wlan security static-wep-key authentication*
- *config wlan security static-wep-key authentication*
- *config wlan security web*
- *config wlan security wpa*

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 WLAN 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]

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	802.1X	802.1X security.
	enable/disable/	Change state command.
	encryption	Sets the static WEP keys and indexes.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.

Defaults (none)

Examples **>config wlan security 802.1X enable foreignAp**

Related Commands show wlan

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	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	cranite	Cranite passthrough.
	enable/disable	Change state command.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.

Defaults (none)

Examples **>config wlan security cranite enable foreignAp**

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	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	fortress	Fortress passthrough.
	enable/disable	Change state command.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.

Defaults (none)

Examples **>config wlan security fortress enable foreignAp**

Related Commands show wlan

config wlan security ipsec

To change the state of the IPSec security, use the config wlan security ipsec command.

>config wlan security ipsec [enable/disable] [<WLAN id>/foreignAp]

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	ipsec	IPSec parameters.
	enable/disable	Change state command.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
Defaults	N/A	
Examples	**>config wlan security IPSec enable foreignAp**	
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.

Use to change the authentication protocol for IPSec to:

- hmac-md5 Enables IPSec HMAC-MD5 authentication.
- hmac-sha-1 Enables IPSec HMAC-SHA-1 authentication.
- none Disables IPSec authentication.

>config wlan security ipsec authentication [hmac-md5/hmac-sha-1/none] [<WLAN id>/foreignAp]

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	ipsec	IPSec security.
	authentication	Authentication parameter.
	[hmac-md5/hmac-sha-1/none]	Authentication protocol.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
Defaults	N/A	
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/des] [<WLAN id>/foreignAp]

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.

	security	Security policy.
	ipsec	IPSec security.
	encryption	Encryption parameter.
	[3des/des]	Encryption protocol.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.

Defaults N/A

Examples **>config wlan security ipsec encryption aes 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	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	ipsec	IPSec security.
	ike	IKE protocol.
	authentication	Authentication parameter.
	certificates	Certificate authentication (no key required).
	pre-share-key	Pre-shared key
	xauth-psk	XAuth pre-shared key.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
	<key>	Key required for pre-share and xauth-psk.

Defaults N/A

Examples **>config wlan security ipsec ike authentication certificates foreignAp**

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-id>

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	ipsec	IPSec security.
	ike	IKE protocol.
	dh-group	Diffie Hellman group parameter.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
	<group-id>	Group 1, 2 or 5

Defaults N/A

Examples **>config wlan security ipsec ike dh-group 1 1**

Related Commands show wlan

config wlan security ipsec ike lifetime

To modify the IPSec IKE timeout used on the wireless LAN, use the config wlan security ipsec ike lifetime command.

>config wlan security ipsec ike lifetime [<WLAN id>/foreignAp] <group-id> <seconds>

Syntax		
	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	ipsec	IPSec security.
	ike	IKE protocol.
	lifetime	IKE timeout.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
	<seconds>	Timeout in seconds

Defaults N/A

Examples **>config wlan security ipsec ike lifetime 1 10**

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		
	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	ipsec	IPSec security.
	ike	IKE protocol.
	phase1	Phase 1 command.
	[aggressive/main]	Phase 1 setting.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.

Defaults N/A

Examples **>config wlan security ipsec ike phase1 aggressive foreignAp**

Related Commands show wlan

config wlan security passthru

To modify Passthru used on the wireless LAN, use the config wlan security ipsec ike passthru command.

>config wlan security passthru [enable/disable] [<WLAN id>/foreignAp]

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	passthru	Passthru command.
	[enable/disable]	Passthru setting.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.

Defaults N/A

Examples **>config wlan security ipsec enable 3 17**

Related Commands show wlan

config wlan security l2tp

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

>config wlan security l3tp [authentication/enable/disable/encryption/ike] [<WLAN id>/foreignAp] [gateway]

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	l2tp	L2tp.
	authentication/	IPSec authentication transform (hmac-md5 or hmac-sha-1).
	enable/disable	Modify l2tp status.
	encryption/	IPSEC configuration transform (3des, aes or des).
	ike	Internal Key Exchange (authentication, DH-Group, lifetime or phase1).
	<WLAN id>	WLAN identifier between 1 and 16.

Defaults N/A

Examples **>config wlan security l2tp enable 1**

Related Commands show wlan

config wlan security static-wep-key

To change the status of static WEP key authentication, use the config wlan security static-wep-key command.

>config wlan security static-wep-key [enable/disable] <WLAN id>

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	static-wep-key	Static WEP key authentication.
	enable/disable	Modify status.
	<WLAN id>	WLAN identifier between 1 and 16.

Defaults N/A

Examples **>config wlan security static-wep-key enable 1**

Related Commands config wlan security wpa encryption

config wlan security static-wep-key authentication

To change the status of static WEP key authentication, use the config wlan security static-wep-key authentication command.

>config wlan security static-wep-key authentication <shared-key/open> <WLAN id>

Syntax		
	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	static-wep-key	Static WEP key authentication.
	authentication	Authentication setting.
	shared-key	Shared-key authentication.
	open	Open authentication.
	<WLAN id>	WLAN identifier between 1 and 16.

Defaults N/A

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 change the status of static WEP key encryption, use the config wlan security static-wep-key encryption command.

Use to enable or disable static wep key encryption. Static WEP encryption parameters:

- Key sizes: 40/64, 104/128 and 128/152 bit key sizes.
- Key Index: 1 to 4.
- Enter encryption key.
- Select encryption key format in ASCII or HEX.

One unique WEP Key Index can be applied to each WLAN. As there are only four WEP Key Indexes, only four WLANs 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		
	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	static-wep-key	Static WEP key authentication.
	encryption	Encryption setting.
	<WLAN id>	WLAN identifier between 1 and 16.
	[40/104/128]	Encryption level.
	hex/ascii	Key format
	<key>	Hex or ASCII key
	<key-index>	Key index

Defaults N/A

Examples **>config wlan security wpa encryption 1 40 hex 0201702001 2**

Related Commands show wlan

config wlan security web

To change the status of Web authentication used on the wireless LAN, use the config wlan security web command.

>config wlan security web [acl/enable/disable] [<WLAN id>/foreignAp] <ACL name/none>

Syntax		
	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	web	Web authentication.
	acl	Add an ACL to the WLAN definition.
	enable/disable	Modify status.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
	<ACL name/none>	Existing ACL name or blank.

Defaults N/A

Examples **>config wlan security web acl 1 ACL03**
>config wlan security web enable
>config wlan security web disable

Related Commands show wlan

config wlan security wpa

To change the status of WPA authentication, use the config wlan security wpa command.

>config wlan security wpa [enable/disable] <WLAN id>

Syntax		
	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	wpa	WPA authentication.
	enable/disable	Modify status.
	<WLAN id>	WLAN identifier between 1 and 16.

Defaults N/A

Examples **>config wlan security wpa enable 1**

Related Commands show wlan

config wlan timeout

To change the timeout of WLAN clients, use the config wlan timeout command.

>config wlan timeout [<WLAN id>/foreignAp] <seconds>

Syntax		
	config	Configure parameters.
	wlan	Wireless LAN parameters.

	timeout	Client timeout.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
	<seconds>	Timeout in seconds.

Defaults N/A

Examples **>config wlan timeout 1 6000**

Related Commands show wlan

config wlan vlan

To add a Virtual LAN, use the config wlan vlan command.

>config wlan vlan [<WLAN id>/foreignAp] [<VLAN id/untagged> [<IP Address> <Netmask> <Gateway>]/default]

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	vlan	Virtual LAN.
	<WLAN id>	WLAN identifier between 1 and 16.
	foreignAp	Third-party access point WLAN 17.
	default	Use the network port configuration
	<VLAN id/untagged>	VLAN ID or untagged
	<IP Address> <Netmask> <Gateway>	If untagged, enter the IP Address, netmask and gateway

Defaults N/A

Examples **>config wlan vlan 1 untagged default**

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	save config	Save Configuration changes.
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, logfiles, and other functions, use the clear commands.

- *clear ap-config*
- *clear arp*
- *clear config*
- *clear stats port*
- *clear stats mobility*
- *clear stats switch*
- *clear redirect-url*
- *clear transfer*
- *clear traplog*
- *clear webimage*
- *clear webmessage*
- *clear webtitle*
- *clear ext-webauth-url*

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 1000 Series lightweight access point>
```

Syntax	clear	Clear.
	ap-config	Cisco 1000 Series lightweight access point configuration.
	<Cisco 1000 Series lightweight access point>	Name of the Cisco 1000 Series lightweight access point.
Defaults	N/A	
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	clear arp	Command action.
Defaults	N/A	

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 remove the Cisco Wireless LAN Controller configuration, use the clear config command.

```
>clear config
```

Syntax

clear	Clear.
config	Cisco Wireless LAN Controller configuration.

Defaults N/A

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

```
>clear stats mobility
```

Syntax

clear	Clear.
stats	Statistics counters.
mobility	Mobility statistics.

Defaults N/A

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

```
>clear stats port <port>
```

Syntax

clear	Clear.
stats	Statistics counters.
port	Port level.

	<port>	Cisco Wireless LAN Controller port.

Defaults N/A

Examples

```
>clear stats port 9
Are you sure you want to clear the port stats? y/n
y
Port 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 switch

To clear all statistics counters on the Cisco Wireless LAN Controller, use the clear stats switch command.

```
>clear stats switch
```

Syntax	clear	Clear.
	stats	Statistics counters.
	switch	Cisco Wireless LAN Controller.

Defaults N/A

Examples

```
>clear stats switch
Are you sure you want to clear the switch stats? y/n
y
Switch stats 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 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	clear redirect-url	Command action.

Defaults N/A

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 transfer information, use the clear transfer command.

>clear transfer

Syntax	clear	Clear.
	transfer	Transfer data.
Defaults	N/A	
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 traplog information, use the clear traplog command.

>clear traplog

Syntax	clear	Clear.
	traplog	Trap logs.
Defaults	N/A	
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	clear webimage	Command action.
Defaults	N/A	
Examples	**>clear webimage** Logo not installed.	
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	clear webmessage	Command action.
Defaults	N/A	
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	clear webtitle	Command action.
Defaults	N/A	
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 custom Web Authentication URL, use the clear ext-webauth-url command.

>clear ext-webauth-url

Syntax	clear URL	Command action.
Defaults	N/A	
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
  - *transfer download certpassword*
  - *transfer download datatype*
  - *transfer download filename*
  - *transfer download mode*
  - *transfer download path*
  - *transfer download serverip*
  - *transfer download start*
  - *transfer download tftpPktTimeout*
  - *transfer download tftpMaxRetries*
- transfer upload
  - *transfer upload datatype*
  - *transfer upload filename*
  - *transfer upload mode*
  - *transfer upload path*
  - *transfer upload serverip*
  - *transfer upload start*

transfer download certpassword

To set a certificate's private password, use the transfer download certpassword command.

>transfer download certpassword [password]

Syntax	transfer	Move a file or configuration.
	download	Download operation to Cisco Wireless LAN Controller.
	certpassword	Certificate's private key password.
	password	Password or blank to clear password.
Defaults	N/A	
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 data type, use the transfer download datatype command.

>transfer download datatype [code/config/webauthcert/webadmincert/image]

Syntax	transfer	Move a file or configuration.
	download	Download operation to Cisco Wireless LAN Controller.
	datatype	Type of data.
	code	Cisco Wireless LAN Controller code.
	config	Configuration file.
	webauthcert	Authentication certificate.
	webadmincert	Administration certificate.
	image	Image

Defaults N/A

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	transfer	Move a file.
	download	Download operation to Cisco Wireless LAN Controller.
	filename <filename>	Enter filename up to 31 alphanumeric characters.

Defaults N/A

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 download a specific file, use the transfer download mode command.

>transfer download mode <mode>

Syntax	transfer	Move a file.
	download mode	Download mode for Cisco Wireless LAN Controller.
	<mode>	Enter mode of tftp.

Defaults N/A

Example **>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 path, use the transfer download path command.

>transfer download path <path>

Syntax	transfer	Move a file.
	download	Download operation for Cisco Wireless LAN Controller.
	path <path>	Enter filename directory path.
Defaults	N/A	
Example	**>transfer download 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 download a specific server, use the transfer download serverip command.

>transfer download serverip <ip addr>

Syntax	transfer	Move a file.
	download	Download operation for Cisco Wireless LAN Controller.
	serverip <IP addr>	Enter IP address of the server.
Defaults	N/A	
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 start a download transfer, use the transfer download start command.

>transfer download start

Syntax	transfer	Move a file.
	download start	Download start operation for Cisco Wireless LAN Controller.
Defaults	N/A	

Example

```
>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 enter the tftp Packet Timeout in secs between 1 and 254, use the transfer download tftpPktTimeout command.

>transfer download tftpPktTimeout <time out>

Syntax	transfer	Move a file
	download tftpPktTimeout	The tftp Packet Timeout in secs between 1 and 254.

Defaults N/A

Example **>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 enter the tftp Packet Max Retries in secs between 1 and 254, use the transfer download tftpMax Timeout command.

>transfer download tftpPktMaxTimeout <time out>

Syntax	transfer	Move a file.
	download tftpPktMaxTimeout	The tftp Packet Maximum timeout in secs between 1 and 254.

Defaults N/A

Example **>transfer download tftpPktMaxTimeout 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 upload datatype

To set the upload data type, use the transfer upload datatype command.

>transfer upload datatype [config/crashfile/errorlog/systemtrace/traplog]

Syntax	transfer	Move a file or configuration.
	upload	Upload operation to Cisco Wireless LAN Controller.

	datatype	Type of data.
	errorlog	Error log file.
	crashfile	Crash file.
	systemtrace	System trace file.
	config	Configuration log.
	traplog	Trap log.

Defaults: N/A

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	transfer	Move a file.
	upload	Upload operation to Cisco Wireless LAN Controller.
	filename <filename>	Enter filename up to 31 alphanumeric characters.

Defaults N/A

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 upload a specific file, use the transfer upload mode command.

>transfer upload mode <mode>

Syntax	transfer	Move a file.
	upload mode	Download mode for Cisco Wireless LAN Controller.
	<mode>	Enter mode of tftp.

Defaults N/A

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	transfer	Move a file.
	upload	Upload operation for Cisco Wireless LAN Controller.
	path <path>	Enter filename directory path up to 31 characters.

Defaults N/A

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 upload a specific server, use the transfer upload serverip command.

>transfer upload serverip <ip addr>

Syntax	transfer	Move a file.
	upload	Upload operation for Cisco Wireless LAN Controller.
	serverip <IP addr>	Enter IP address of the server.

Defaults N/A

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 start an upload transfer, use the transfer upload start command.

>transfer download start

Syntax	transfer	Move a file.
	upload start	Download start operation for Cisco Wireless LAN Controller.

Defaults N/A

Examples

```
>transfer upload 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 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 Technical Assistance Center (TAC) personnel. Please do not use these commands without direction from the Cisco Technical Assistance Center (TAC).