



Cisco WLAN Solution CLI Reference

System Release 3.0

The Cisco WLAN Solution command line interface (CLI) allows operators to connect an ASCII console to the Cisco Wireless LAN Controller and configure the Cisco Wireless LAN Controller and its associated Cisco 1000 Series lightweight access points using the command line interface. The [Using the Cisco WLAN Solution 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 Cisco Wireless LAN Controller or reset configuration to factory defaults.

Config

Configure Cisco Wireless LAN Controller 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 Cisco Wireless LAN Controller settings to Non-volatile RAM.

Show

Display Cisco Wireless LAN Controller options and settings.

Transfer

Transfer a file to or from the Cisco Wireless LAN Controller.

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 acl*](#)
- [*show advanced 802.11a*](#)
- [*show advanced 802.11b*](#)
- [*show advanced client-handoff*](#)
- [*show advanced statistics*](#)
- [*show ap*](#)
- [*show arp switch*](#)
- [*show exclusionlist*](#)
- [*show boot*](#)
- [*show certificate*](#)
- [*show client*](#)
- [*show country*](#)
- [*show cpu*](#)
- [*show custom-web*](#)
- [*show database*](#)
- [*show debug*](#)
- [*show dhcp*](#)
- [*show dhcp summary*](#)
- [*show eventlog*](#)
- [*show ike*](#)
- [*show ipsec*](#)
- [*show interface*](#)
- [*show inventory*](#)
- [*show l2tp*](#)
- [*show load-balancing*](#)
- [*show login session*](#)
- [*show known*](#)
- [*show location*](#)
- [*show macfilter*](#)
- [*show mgmtuser*](#)
- [*show mesh*](#)
- [*show mobility statistics*](#)

- [show mobility summary](#)
- [show msglog](#)
- [show nac statistics](#)
- [show nac summary](#)
- [show netuser](#)
- [show network](#)
- [show port](#)
- [show pmk-cache](#)
- [show qos queue length all](#)
- [show radius](#)
- [show rfid config](#)
- [show rfid detail](#)
- [show rfid summary](#)
- [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 time](#)
- [show trapflags](#)

- [show traplog](#)
- [show watchlist](#)
- [show wlan](#)
- [show wlan summary](#)

show 802.11a

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

>show 802.11a

Syntax	show 802.11a	Display configurations. 802.11a configurations.
Defaults	(none)	
Examples	>show 802.11a <pre> 802.11a Network..... Enabled 802.11a Low Band..... Enabled 802.11a Mid Band..... Enabled 802.11a High Band..... Enabled 802.11a Operational Rates 802.11a 6M Rate..... Mandatory 802.11a 9M Rate..... Supported 802.11a 12M Rate..... Mandatory 802.11a 18M Rate..... Supported 802.11a 24M Rate..... Mandatory 802.11a 36M Rate..... Supported 802.11a 48M Rate..... Supported 802.11a 54M Rate..... Supported Beacon Interval..... 100 CF Pollable mandatory..... Disabled CF Poll Request mandatory..... Disabled CFP Period..... 4 CFP Maximum Duration..... 100 Default Channel..... 36 Default Tx Power Level..... 1 DTIM Period..... 10 Fragmentation Threshold..... 2346 Long Retry Limit..... 4 Maximum Rx Life Time..... 512 Max Tx MSDU Life Time..... 512 Medium Occupancy Limit..... 100 Pico-Cell Status..... Disabled RTS Threshold..... 2347 Short Retry Limit..... 7 TI Threshold..... -50 </pre>	
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 802.11b	Display configurations. 802.11b/g configurations.
Defaults	(none)	
Examples	<pre> >show 802.11b 802.11b Network..... Enabled 11gSupport..... Disabled 802.11b Operational Rates 802.11b/g 1M Rate..... Mandatory 802.11b/g 2M Rate..... Mandatory 802.11b/g 5.5M Rate..... Mandatory 802.11b/g 11M Rate..... Mandatory 802.11b/g 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 RTS Threshold..... 2347 Short Preamble mandatory..... Enabled Short Retry Limit..... 7 </pre>	

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

show acl

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

>show acl [summary/detailed]

Syntax	show acl summary detailed	Command action. Display a summary of the Access Control Lists. 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 receiver*](#)
- [*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
Related Commands	802.11a Last Run.....	133 seconds ago
	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 receiver

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

>show advanced 802.11a receiver

Syntax	show	Display configurations.
	advanced	Advanced parameters.
	802.11a	802.11a network.
	receiver	Receiver.
Defaults	(none)	
Examples	>show advanced 802.11a receiver	
	<pre> 802.11a Advanced Receiver Settings RxStart : Signal Threshold..... 15 RxStart : Signal Lamp Threshold..... 5 RxStart : Preamble Power Threshold..... 2 RxReStart : Signal Jump Status..... Enabled RxReStart : Signal Jump Threshold..... 10 TxStomp : Low RSSI Status..... Enabled TxStomp : Low RSSI Threshold..... 30 TxStomp : Wrong BSSID Status..... Enabled TxStomp : Wrong BSSID Data Only Status..... Enabled RxAbort : Raw Power Drop Status..... Disabled RxAbort : Raw Power Drop Threshold..... 10 RxAbort : Low RSSI Status..... Disabled RxAbort : Low RSSI Threshold..... 0 RxAbort : Wrong BSSID Status..... Disabled RxAbort : Wrong Data Only Status..... Disabled </pre>	
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.
	Transmit Power Assignment Leader.....	a5:6b:ac:10:01:6b
Related Commands	Last Run..... 384 seconds ago	
	config advanced 802.11a txpower-update, config 802.11a txPower	

show advanced 802.11a profile

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

```
>show advanced 802.11a profile global
>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	<pre>>show advanced 802.11a profile global Default 802.11a Cell performance profiles 802.11a Global Interference threshold..... 10% 802.11a Global noise threshold..... -70 dBm 802.11a Global RF utilization threshold..... 80% 802.11a Global throughput threshold..... 1000000 bps 802.11a Global clients threshold..... 12 clients 802.11a Global coverage threshold..... 12 dB 802.11a Global coverage exception level..... 80% 802.11a Global client minimum exception lev..... 3 clients >show advanced 802.11a profile AP1 Cisco 1000 Series lightweight access point performance profile not customized This response indicates that the performance profile for this Cisco 1000 Series lightweight access point is using the global defaults and has not been individu- ally configured.</pre>
-----------------	--

Related Commands	config advanced 802.11b profile clients, config advanced 802.11b profile coverage, config advanced 802.11b profile customize, config advanced 802.11b profile exception, config advanced 802.11b profile foreign, config advanced 802.11b profile level, config advanced 802.11b profile noise, config advanced 802.11b profile throughput, config advanced 802.11b profile utilization
-------------------------	---

show advanced 802.11a summary

To display the advanced 802.11a Cisco 1000 Series lightweight access point name, channel, and transmit level summary, use the show advanced 802.11a summary command.

>show advanced 802.11a summary

Syntax	show	Display configurations.
	advanced	Advanced parameters.
	802.11a	802.11a network.
	summary	Cisco 1000 Series lightweight access point name, channel, and transmit level summary.

Defaults (none)

Examples **>show advanced 802.11a summary**

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

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
Related Commands	802.11b Last Run.....	511 seconds ago
	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
Transmit Power Update Logging..... Off
```

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

show advanced 802.11b monitor

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

>show advanced 802.11b monitor

Syntax	show advanced 802.11b monitor	Display configurations. Advanced parameters. 802.11b/g network. 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
RxAabort  : Raw Power Drop Status..... Disabled
RxAabort  : Raw Power Drop Threshold..... 0
RxAabort  : Low RSSI Status..... Enabled
RxAabort  : Low RSSI Threshold..... 0
RxAabort  : Wrong BSSID Status..... Disabled
RxAabort  : 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 advanced 802.11b profile	Display configurations. Advanced parameters. 802.11b/g network. Cisco 1000 Series lightweight access point performance profile.
---------------	--	--

Defaults	(none)
-----------------	--------

Examples	<pre>>show advanced 802.11b profile global Default 802.11b Cell performance profiles 802.11b Global Interference threshold..... 10% 802.11b Global noise threshold..... -70 dBm 802.11b Global RF utilization threshold..... 80% 802.11b Global throughput threshold..... 1000000 bps 802.11b Global clients threshold..... 12 clients 802.11b Global coverage threshold..... 12 dB 802.11b Global coverage exception level..... 80% 802.11b Global client minimum exception lev..... 3 clients >show advanced 802.11b profile AP1 Cisco 1000 Series lightweight access point performance profile not customized This response indicates that the performance profile for this Cisco 1000 Series lightweight access point is using the global defaults and has not been individually configured.</pre>
-----------------	---

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
Related Commands	Last Run..... 427 seconds ago	
	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	Cisco 1000 Series lightweight access point name, channel, and transmit level summary.

Defaults (none)

Examples **>show advanced 802.11b summary**

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

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 access point 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 a 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 Identifier..... 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 Location..... default location
Primary Cisco WLAN Solution Switch..... Pubs
Secondary Cisco WLAN Solution Switch.....
Tertiary Cisco WLAN Solution 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 Identifier..... 5

```

```

Cisco 1000 Series lightweight access point
Name..... AP01
AP Type..... Cisco WLAN Solution
Switch Port Number..... 19
MAC Address..... 00:0b:85:01:05:00
IP Address..... Disabled
Cisco 1000 Series lightweight access point Location..... default location
Primary Cisco WLAN Solution Switch.....
Secondary Cisco WLAN Solution Switch.....
Tertiary Cisco WLAN Solution 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 AP Identifier..... 5

Name..... AP01
AP Type..... Cisco WLAN Solution
Switch Port Number..... 19
MAC Address..... 00:0b:85:01:05:00
IP Address..... Disabled
Cisco 1000 Series lightweight access point Location..... 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 a 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 Cisco 1000 Series lightweight access points attached to the Cisco Wireless LAN Controller, use the show ap summary command. A list containing each Cisco 1000 Series lightweight access point name, number of slots, manufacturer, MAC address, location and Cisco Wireless LAN Controller port number is displayed.

>show ap summary

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

Defaults	(none)
-----------------	--------

Examples	>show ap summary <table border="1"> <thead> <tr> <th>AP Name</th> <th>Slots</th> <th>AP Type</th> <th>MAC Addr</th> <th>Location</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td>AP03 location 12</td> <td>2</td> <td>Cisco WLAN Solution</td> <td>00:0b:85:01:18:b0</td> <td>default</td> <td></td> </tr> <tr> <td>AP02 location 11</td> <td>2</td> <td>Cisco WLAN Solution</td> <td>00:0b:85:01:12:60</td> <td>default</td> <td></td> </tr> <tr> <td>AP01 location 19</td> <td>2</td> <td>Cisco WLAN Solution</td> <td>00:0b:85:01:05:00</td> <td>default</td> <td></td> </tr> </tbody> </table>	AP Name	Slots	AP Type	MAC Addr	Location	Port	AP03 location 12	2	Cisco WLAN Solution	00:0b:85:01:18:b0	default		AP02 location 11	2	Cisco WLAN Solution	00:0b:85:01:12:60	default		AP01 location 19	2	Cisco WLAN Solution	00:0b:85:01:05:00	default	
AP Name	Slots	AP Type	MAC Addr	Location	Port																				
AP03 location 12	2	Cisco WLAN Solution	00:0b:85:01:18:b0	default																					
AP02 location 11	2	Cisco WLAN Solution	00:0b:85:01:12:60	default																					
AP01 location 19	2	Cisco WLAN Solution	00:0b:85:01:05:00	default																					

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 Cisco 1000 Series lightweight access points.
	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 arp switch	Display configurations. arp MAC addresses, IP Addresses, and port types. 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.

>show exclusionlist

Syntax	show exclusionlist	Display configurations. Manual Exclusion List.
Defaults	(none)	
Examples	<pre>>show exclusionlist MAC Address Description ----- 00:50:08:00:00:f5 Disallowed Client</pre>	
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 boot	Display configurations. 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 a Cisco 1000 Series lightweight access point, use the show client ap command.

► **Note:** The show client ap command may list the status of automatically disabled clients. Use the **show exclusionlist** command to view clients on the Exclusion List (blacklisted).

>show client ap <802.11a/802.11b> <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 exclusionlist

show client detail

To display detailed information for a client on a Cisco 1000 Series lightweight access point, use the show client detail command.

► **Note:** The show client ap command may list the status of automatically disabled clients. Use the **show exclusionlist** command to view clients on the Exclusion List (blacklisted).

>show client detail <MAC 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 (DSCP)..... disabled
802.1P Priority Tag..... disabled
Mobility State..... Local
Mobility Move Count..... 0
Security Policy Completed..... No
Policy Manager State..... DHCP_REQD
Policy Manager Rule Created..... No
NPU Fast Notified..... Yes
Policy Type..... N/A
Encryption Cipher..... WEP (104 bits)
EAP Type..... Unknown
Interface..... management
VLAN..... 0
Client Capabilities:
  CF Pollable..... Not implemented
  CF Poll Request..... Not implemented
  Short Preamble..... Not implemented
  PBCC..... Not implemented
  Channel Agility..... Not implemented
  Listen Interval..... 0
Client Statistics:
  Number of Bytes Received..... 0
  Number of Bytes Sent..... 0
  Number of Packets Received..... 0
  Number of Packets Sent..... 0
  Number of Policy Errors..... 0
  Radio Signal Strength Indicator..... Unavailable
  Signal to Noise Ratio..... Unavailable
```



Nearby AP Statistics:

AP03(slot 0) 24643 seconds ago..... -11 dBm

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

show client summary

To display a summary of clients associated with a Cisco 1000 Series lightweight access point, use the `show client summary` command.

► **Note:** The `show client ap` command may list the status of automatically disabled clients. Use the `show exclusionlist` command to view clients on the Exclusion List (blacklisted).

>show client summary

Syntax	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 exclusionlist						

show client username

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

>show client username <User Name>

Syntax	show	Display configurations.			
	username	Cisco Radio.			
	<User Name>	Client User Name.			
Defaults	(none)				
Examples	>show client username IT_007				
	MAC Address	AP ID	Status	WLAN Id	Authenticated
	-----	-----	-----	-----	-----
	00:0c:41:0a:33:13	1	Associated	1	No
Related Commands	show client ap, show client detail, show client summary				

show country

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

► **Note:** Refer to [Cisco WLAN Solution Supported Country Codes](#) in the [Product Guide](#) for the most recent country codes and regulatory domains.

>show country

Syntax	show country	Display configuration options. Supported Countries.
---------------	-----------------	--

Defaults	(none)
-----------------	--------

Examples	>show country Supported Country Codes
-----------------	--

```

AR..... 802.11a/802.11b
AT..... 802.11a/802.11b/802.11g
AU..... 802.11a/802.11b/802.11g
BR..... 802.11a/802.11b
BE..... 802.11a/802.11b/802.11g
CA..... 802.11a/802.11b/802.11g
CH..... 802.11a/802.11b/802.11g
CY..... 802.11a/802.11b/802.11g
CZ..... 802.11a/802.11b
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
IL..... 802.11a/802.11b
ILO..... 802.11a/802.11b
IT..... 802.11a/802.11b/802.11g
JP..... 802.11a/802.11b/802.11g
KR..... 802.11a/802.11b
LT..... 802.11a/802.11b/802.11g
LV..... 802.11a/802.11b
MA..... 802.11a
MX..... 802.11a/802.11b/802.11g
MY..... 802.11a
NL..... 802.11a/802.11b/802.11g
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
SA..... 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)
```

Related Commands show sysinfo

show database

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

>show database summary

Syntax	show database. summary	Command action. Database summary.
Defaults	(none)	
Examples	>show database summary Current Max database entries..... 512 Max database entries on next reboot..... 512	
Related Commands	show sysinfo	

show cpu

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

>show cpu

Syntax	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	<pre>>show custom-web Cisco WLAN Solution Logo..... Enabled CustomLogo..... Disabled Custom Title..... Disabled Custom Message..... Disabled Custom Redirect URL..... Disabled External Web Authentication Mode..... Disabled External Web Authentication URL..... Disabled</pre>	
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 debug	Display configurations. MAC address debugging.
Defaults	disabled	
Examples	>show debug MAC debugging..... disabled Debug Flags Enabled: arp error enabled. bcast error enabled.	
Related Commands	debug mac	

show dhcp

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

>show dhcp <scope name>

Syntax	show dhcp <scope name>	Command action. The scope name set with the config dhcp command.
Defaults	None	
Examples	<pre> >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 </pre>	
Related Commands	config dhcp, show dhcp summary	

show dhcp summary

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

>show dhcp summary

Syntax	show dhcp summary	Command action. List information about internal 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	Time
					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 inventory	Display configurations. Physical Cisco Wireless LAN Controller configuration.
Defaults	(none)	
Examples	>show inventory Switch Description..... Machine Model..... 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 Cisco 1000 Series lightweight access point information, use the show known command.

>show known ap <summary/detailed>

Syntax	show	Display configurations.				
	known ap	Known Cisco 1000 Series lightweight access point information.				
	<summary/	Displays a list of all Known Cisco 1000 Series lightweight access points.				
	detailed>	Provides detailed information for a Known Cisco 1000 Series lightweight access point.				
Defaults	None					
Examples	>show known ap summary					
	MAC Address	State	# APs	# Clients	Last Heard	
	-----	-----	-----	-----	-----	
Related Commands	config ap					

show location

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

>show location summary

Syntax	show location	Display command for locations.
	<summary/	Displays status of locations
Defaults	None	
Examples	>show location summary	
	Status..... disabled	
Related Commands	config location	

show load-balancing

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

>show load-balancing

Syntax	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 login session

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

>show login session

Syntax	show	Display configurations.		
	login session	Current session details.		
Defaults	(none)			
Examples	>show login session			
	ID	User Name	Connection From	Idle Time
	---	-----	-----	-----
	00	admin	172.18.4.84	00:00:00
Related Commands	01:08:18			
	config login session 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	
Related Commands	Unable to retrieve MAC filter.	
	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 mgmtuser	Display configurations. Management users.	
Defaults	(none)		
Examples	>show mgmtuser		
	User Name	Permissions	Description
	-----	-----	-----
	admin	read-write	
Related Commands	config mgmtuser add, config mgmtuser delete, config mgmtuser password		

show mesh

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

>show mesh <neigh/path/stats/linkrate/summary>

Syntax	show	Display configurations.
	mesh	Mesh configuration.
	<neigh/	Cisco 1000 Series lightweight access point neighborhood list.
	path/	Cisco 1000 Series lightweight access point path.
	stats/	Cisco 1000 Series lightweight access point statistics
	linkrate/	Link rate statistics
	summary>	Link rate neighborhood summary.
Defaults	(none)	
Examples	>show mesh summary	
	TBD	
Related Commands	config mesh	

SHOW MOBILITY COMMANDS

Use the following show mobility commands.

- [*show mobility statistics*](#)
- [*show mobility anchor*](#)
- [*show mobility summary*](#)

show mobility statistics

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

>show mobility statistics

Syntax	show	Display configurations.
	mobility	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 anchor

To display the WLAN anchor list for the Cisco Wireless LAN Controller mobility groups, use the show mobility anchor command.

>show mobility anchor

Syntax	show	Display configurations.
	mobility	Mobility group.
	anchor	Anchor list.
Defaults	(none)	
Examples	>show mobility anchor	
	Mobility Anchor Export List	
	WLAN ID	IP Address
Related Commands	config mobility group discovery, config mobility group member	

show mobility summary

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

>show mobility summary

Syntax	show mobility summary	Display configurations. Mobility group. Summary details
Defaults	(none)	
Examples	>show mobility summary Mobility Protocol Port..... 16666 Mobility Security Mode..... Disabled Default Mobility Domain..... default 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 than 15 entries you are prompted to display the messages shown in the example.

	>show msglog	
Syntax	show msglog	Display configurations. 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 mobility summary

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

>show mobility summary

Syntax	show mobility summary	Display configurations. Mobility group. Summary details
Defaults	(none)	
Examples	>show mobility summary Mobility Protocol Port..... 16666 Mobility Security Mode..... Disabled Default Mobility Domain..... default 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 nac statistics

To display Network Access Control detailed information about a Cisco Wireless LAN Controller, use the show nac statistics command.

>show nac statistics

Syntax	show	Display configurations.
	nac	Network Access Control.
	statistics	Detailed statistics.
Defaults	(none)	
Examples	>show nac statistics	
	Server Index.....	1
	Server Address.....	1.1.1.1
	Number of requests sent.....	0
	Number of retransmissions.....	0
	Number of requests received.....	0
	Number of malformed requests received.....	0
	Number of bad auth requests received.....	0
	Number of pending requests.....	0
	Number of timed out requests.....	0
	Number of misc dropped request received.....	0
	Number of requests sent.....	0
Related Commands	show nac acl, show nac summary.	

show nac summary

To display Network Access Control summary information for a Cisco Wireless LAN Controller, use the show nac summary command.

>show nac summary

Syntax	show nac summary	Display configurations. Network Access Control. Summary information
Defaults	(none)	
Examples	>show nac summary NAC ACL Name Index Server Address Port State ----- 1 1.1.1.1 13336 Enabled	
Related Commands	show nac acl, show nac statistics.	

show netuser

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

>show netuser

Syntax	show netuser	Display configurations. Network users.									
Defaults	(none)										
Examples	>show netuser <table> <thead> <tr> <th>User Name</th><th>WLAN Id</th><th>Description</th></tr> </thead> <tbody> <tr> <td>-----</td><td>-----</td><td>-----</td></tr> <tr> <td>krebbis</td><td>1</td><td>all krebbis</td></tr> </tbody> </table>		User Name	WLAN Id	Description	-----	-----	-----	krebbis	1	all krebbis
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 network	Display configurations. 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 ARP Unicast Mode..... Disabled 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..... 80 Fast SSID Change..... Disabled	
Related Commands	config network arptimeout, config network bcast-ssid, config network dsport, config network master-base, config network mgmt-via-wireless, config network params, config network rf-mobility-domain, config network secureweb, config network secweb-passwd, config network ssh, config network telnet, config network usertimeout, config network vlan, config network webmode	

show port

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

```
>show port <port number>
```

```
>show port summary
```

Syntax

```
show port <port number>/summary
```

Display configurations.
Cisco Wireless LAN Controller port.
Individual port or all ports

Defaults (none)

Examples

```
>show port 7
```

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

```
>show port summary
```

Pr	Type	STP Stat	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	Mcast 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 queue_length all	Command action Display all quality of service queue lengths.
---------------	------------------------------	---

Defaults	(none)
-----------------	--------

Examples	<pre>>show qos queue_length all Platinum queue length..... 255 Gold queue length..... 255 Silver queue length..... 150 Bronze queue length..... 100</pre>
-----------------	--

Related Commands	config qos
-------------------------	------------

show pmk-cache

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

```
>show pmk-cache [summary/all/<MAC addr>]
```

Syntax	show	Display configurations.
	pmk-cache	PMK cache
	[summary/all/<MAC addr>]	Summary, all, or for a specific MAC address

Defaults	(none)
-----------------	--------

Examples	>show pmk-cache summary
	PMK Cache
	Station Remaining Lifetime

Related Commands	config pmk-cache delete
-------------------------	-------------------------

show rfid config

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

>show rfid config

Syntax	show	Display configurations.
	rfid	Network configuration.
	<config	Configuration options for RFID tracking system
Defaults	(none)	
Examples	>show rfid config	
	RFID Tag data Collection..... Enabled	
	RRID Tag Auto-Timeout..... Enable	
	RFID Client data Collection..... Disabled	
	RFID data timeout..... 1200 seconds	
Related Commands	config rfid, show rfid summary, show rfid detail.	

show rfid detail

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

>show rfid detail <MAC address>

Syntax	show	Display configurations.
	rfid	Network configuration.
	detail	Detailed information for one rfid tag
Defaults	(none)	
Examples	>show rfid detail 00:40:96:90:d1:6a	
	TBD	
Related Commands	config rfid, show rfid config, show rfid summary.	

show rfid summary

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

>show rfid summary

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

Defaults	(none)
-----------------	--------

Examples	>show rfid summary
	RFID TYPE Closest AP RSSI Time Since Last Heard

Related Commands	config rfid, show rfid config, show rfid detail.
-------------------------	--

SHOW RADIUS COMMANDS

Use the following show radius commands:

- [*show radius acct statistics*](#)
- [*show radius auth statistics*](#)
- [*show radius rfc3576*](#)
- [*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 statistics	RADIUS accounting server. Statistics
Defaults	(none)	
Examples	>show radius acct statistics	
	Accounting Servers:	
	Server Index.....	1
	Server Address.....	10.1.17.10
	Msg Round Trip Time.....	0 (1/100 second)
	First Requests.....	0
	Retry Requests.....	0
	Accounting Responses.....	0
	Malformed Msgs.....	0
	Bad Authenticator Msgs.....	0
	Pending Requests.....	0
	Timeout Requests.....	0
	Unknowntype Msgs.....	0
	Other Drops.....	0
Related Commands	show radius auth statistics, show radius summary	

show radius auth statistics

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

>show radius auth statistics

Syntax	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
	Unknown type Msgs.....	0
	Other Drops.....	0
Related Commands	show radius acct statistics, show radius summary	

show radius rfc3576

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

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

	>show radius rfc3576 statistics	
Syntax	show	Display configurations.
	radius rfc3576	RADIUS RFC3576 server
Defaults	(none)	
Examples	>show radius rfc3576 statistics	
	RFC-3576 Servers: Server Index..... 1 Server Address..... 10.1.17.10 Msg Round Trip Time..... 0 (1/100 second) First Requests..... 0 Retry Requests..... 0 Accounting Responses..... 0 Malformed Msgs..... 0 Bad Authenticator Msgs..... 0 Pending Requests..... 0 Timeout Requests..... 0 Unknown type Msgs..... 0 Other Drops..... 0	
Related Commands	show radius auth statistics, show radius summary, show radius rfc3576	

show radius summary

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

>show radius summary

Syntax	show radius summary	Display configurations. RADIUS authentication server. 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 access point 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 point.
	clients	Summary information.
	<Rogue AP MAC address>	Rogue access point 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 point.
	detailed	Summary information.
	<MAC address>	Rogue access point 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 point.
	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 Ad Hoc commands:

- [*show rogue adhoc detailed*](#)
- [*show rogue adhoc summary*](#)

show rogue adhoc detailed

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

>show rogue adhoc detailed <Adhoc Rogue MAC address>

Syntax	show	Display configurations.
	rogue adhoc	Ad hoc Rogue.
	detailed	Summary information.
	<MAC address>	Ad hoc Rogue MAC address.

Defaults (none)

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

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

Related Commands show rogue adhoc summary

show rogue adhoc summary

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

>show rogue adhoc summary

Syntax	show	Display configurations.
	rogue adhoc	Adhoc rogue access point.
	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 a 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 summary	Command action Summary information.										
Defaults	(none)											
Examples	>show route summary Number of Routes..... 1 <table><tr><td>Destination Network</td><td>Genmask</td><td>Gateway</td></tr><tr><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>193.122.17.3</td><td>255.255.255.0</td><td>172.99.3.89</td></tr></table>			Destination Network	Genmask	Gateway	-----	-----	-----	193.122.17.3	255.255.255.0	172.99.3.89
Destination Network	Genmask	Gateway										
-----	-----	-----										
193.122.17.3	255.255.255.0	172.99.3.89										
Related Commands	config route											

show rules

To 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 show a comprehensive view of 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
Switch Description..... Cisco 1000 Series light-
weight access point
Machine Model..... (UNUSED PRODUCT)
Serial Number..... 01012403-10037905-01007
Burned-in MAC Address..... 00:0B:85:02:0D:20
Gig Ethernet/Fiber Card..... Present
Crypto Accelerator..... Present
Press Enter to continue
System Information
Manufacturer's Name..... Cisco WLAN Solution
Product Name..... Cisco 1000 Series light-
weight access point
Product Version..... 3.0.133.0
RTOS Version..... 3.0.133.0
Bootloader Version..... 3.0.133.0

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
Press Enter to continue
Switch Configuration
802.3x Flow Control Mode..... Enable
Current LWAPP Transport Mode..... Layer 2
LWAPP Transport Mode after next switch reboot.... Layer 2
Press Enter to continue
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
ARP Unicast Mode..... Disabled
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
Fast SSID Change..... Disabled
Press Enter to continue

```

Port Summary

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

Press Enter to continue

AP Summary

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

Press Enter to continue. . .

Related Commands

config route

show serial

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

>show serial

Syntax	show serial	Display configurations. Console serial port.
Defaults	9600, 8, OFF, 1, (none)	
Examples	<pre>>show serial Serial Port Login Timeout (minutes)..... 0 Baud Rate..... 9600 Character Size..... 8 Flow Control:..... Disable Stop Bits..... 1 Parity Type:..... none</pre>	
Related Commands	config serial baudrate, config serial timeout	

show sessions

To show the console port login timeout and maximum number of simultaneous CLI sessions, use the `show sessions` command.

>show sessions

Syntax	<code>show sessions</code>	Display configurations. CLI session limits.
Defaults	5 minutes, 5 sessions.	
Examples	<pre>>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.</pre>	
Related Commands	<code>config sessions maxsessions</code> , <code>config sessions timeout</code>	

show snmpcommunity

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

>show snmpcommunity

Syntax	show snmpcommunity	Display configurations. SNMP version 1/version 2c community configuration.
Defaults	(none)	
Examples	<pre>>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</pre>	
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 snmptrap	Display configurations. SNMP trap receivers.									
Defaults	(none)										
Examples	>show snmptrap <table> <tr> <th>SNMP Trap Receiver Name</th><th>IP Address</th><th>Status</th></tr> <tr> <td>-----</td><td>-----</td><td>-----</td></tr> <tr> <td>180.16.19.81</td><td>172.16.16.81</td><td>Enable</td></tr> </table>		SNMP Trap Receiver Name	IP Address	Status	-----	-----	-----	180.16.19.81	172.16.16.81	Enable
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 snmpv3user	Display configurations. SNMP version 3 configuration.												
Defaults	(none)													
Examples	>show snmpv3user <table><tr><td>SNMP v3 User Name</td><td>AccessMode</td><td>Authentication</td><td>Encryption</td></tr><tr><td>-----</td><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>default</td><td>Read/Write</td><td>HMAC-MD5</td><td>CBC-DES</td></tr></table>		SNMP v3 User Name	AccessMode	Authentication	Encryption	-----	-----	-----	-----	default	Read/Write	HMAC-MD5	CBC-DES
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 show the SNMP version status, use the show snmpversion command.

>show snmpversion

Syntax	show snmpversion	Display configurations. 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 show the Cisco Wireless LAN Controller spanning tree port configuration, use the show spanningtree port command.

► **Note:** When the a Cisco 4400 Series Wireless LAN Controller is configured for port redundancy, spanning tree protocol must be disabled for all ports on the Cisco 4400 Series Wireless LAN Controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 Series Wireless LAN Controller.

>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 - 1 or 2 on Cisco 4402 Series Wireless LAN Controller - 1 through 4 on Cisco 4404 Series Wireless LAN Controller
Defaults	800C, Disabled, 802.1D, 128, 100, Auto.	
Examples	>show spanningtree port 3	
	STP Port ID.....	800C
	STP Port State.....	Disabled
	STP Port Administrative Mode.....	802.1D
	STP Port Priority.....	128
	STP Port Path Cost.....	100
Related Commands	STP Port Path Cost Mode.....	Auto
	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 spanningtree switch <port>	Display configurations. Spanning tree. Cisco Wireless LAN Controller configuration. Physical port number: - 1 through 4 on Cisco 2000 Series Wireless LAN Controller - 1 or 2 on Cisco 4100 Series Wireless LAN Controller - 1 or 2 on Cisco 4402 Series Wireless LAN Controller - 1 through 4 on Cisco 4404 Series Wireless LAN Controller
Defaults	(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
		- 1 or 2 on Cisco 4402 Series Wireless LAN Controller
		- 1 through 4 on Cisco 4404 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 switchconfig	Display configurations. 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 sysinfo	Display configurations. Cisco Wireless LAN Controller information.
Defaults	(none)	
Examples	<pre> >show sysinfo Manufacturer's Name..... <company name> Product Name..... Product Version..... 1.2.48.0 RTOS Version..... 1.2.48.0 Bootloader Version..... 1.1.11.0 System Name..... IT2003 System Location..... Andrew 1 System Contact..... Wireless_administrator System ObjectID..... 1.3.6.1.4.1.14179 IP Address..... 172.168.2.36 System Up Time..... 2 days 11 hrs 30 mins 1 secs Configured Country..... United States Operating Environment..... Commercial (0 to 40 C) Internal Temp Alarm Limits..... 0 to 65 C Internal Temperature..... +38 C State of 802.11b Network..... Enabled State of 802.11a Network..... Enabled Number of WLANs..... 2 3rd Party Access Point Support..... Disabled Number of Active Clients..... 1 </pre>	
Related Commands	config country, config wlan, config ap	

show syslog

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

>show syslog

Syntax	show syslog	Display configurations. 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 tech-support	Display configurations. 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 time	Display configurations. Cisco Wireless LAN Controller time and date.
Defaults	(none)	
Examples	<pre> >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 ----- </pre>	
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 trapflags	Display configurations. Cisco Wireless LAN Controller SNMP trap flags.
Defaults	(none)	
Examples	<pre> >show trapflags Authentication Flag..... Enable Link Up/Down Flag..... Enable Multiple Users Flag..... Enable Spanning Tree Flag..... Enable Client Related Traps 802.11 Disassociation..... Disable 802.11 Deauthenticate..... Disable 802.11 Authenticate Failure..... Disable 802.11 Association Failure..... Disable Excluded..... Disable 802.11 Security related traps WEP Decrypt Error..... Enable Cisco WLAN Solution AP Register..... Enable InterfaceUp..... Enable Auto-RF Profiles Load..... Enable Noise..... Enable Interference..... Enable Coverage..... Enable Auto-RF Thresholds tx-power..... Enable channel..... Enable antenna..... Enable AAA auth..... Enable servers..... Enable rogueap..... Enable wps..... Enable configsave..... Enable IP Security esp-auth..... Enable esp-replay..... Enable invalidSPI..... Enable ike-neg..... Enable suite-neg..... Enable invalid-cookie..... Enable </pre>	

Related Commands

config trapflags authentication, config trapflags linkmode, config trapflags multiusers, config trapflags stpmode, config trapflags client, config trapflags ap, config trapflags rrm-profile, config trapflags rrm-params, config trapflags aaa, config trapflags rogueap, config trapflags configsave, config trapflags ipsec, show traplog

show traplog

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

>show traplog

Syntax 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:00:0b:85:01:18:b0 Interface no:1(unknown type)
1	Sun Aug 10 03:10:06 2003	Rogue AP: 00:0b:85:01:02:40 removed from AP:00:0b:85:01:18:b0 Interface no:1(unknown type)
2	Sun Aug 10 03:10:06 2003	Rogue AP: 00:0b:85:01:4c:90 removed from AP:00:0b:85:01:18:b0 Interface no:1(unknown type)
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 watchlist	Command action. 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>

Syntax	show wlan summary <WLAN id>	Display configurations. Wireless LAN. Displays a summary of all WLANs. Cisco WLAN Solution WLAN 1 through 16.
Defaults	(none)	
Examples	>show wlan 1 <pre> WLAN Identifier..... 1 Network Name (SSID)..... Controller Status..... Enabled MAC Filtering..... Disabled AAA Policy Override..... Disabled Network Access Control..... Disabled Number of Active Clients..... 1 Exclusionlist..... Disabled Session Timeout..... Infinity Interface..... management DHCP Server..... 10.1.2.119 Quality of Service..... Bronze (low) WMM..... Allowed 802.11e..... Disabled Wired Protocol..... None IPv6..... Disabled Radio Policy..... All Security 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 (WPA1)..... Disabled Wi-Fi Protected Access v2 (WPA2)..... Disabled IP Security..... Disabled IP Security Passthru..... Disabled L2TP..... Disabled Web Based Authentication..... Disabled Cranite Passthru..... Disabled Fortress Passthru..... Disabled </pre>	
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 wlan summary	Display configurations. Wireless LAN. Cisco Wireless LAN Controller Virtual Gateway IP Address.
---------------	-------------------------	--

Defaults	(none)
-----------------	--------

Examples	>show wlan summary <table> <tr> <th>WLAN ID</th> <th>WLAN Name</th> <th>Status</th> </tr> <tr> <td>1</td> <td>Controller</td> <td>Enabled</td> </tr> <tr> <td>2</td> <td>Marketing</td> <td>Enabled</td> </tr> </table>	WLAN ID	WLAN Name	Status	1	Controller	Enabled	2	Marketing	Enabled
WLAN ID	WLAN Name	Status								
1	Controller	Enabled								
2	Marketing	Enabled								

Related Commands	config wlan summary
-------------------------	---------------------

Setting Configurations

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

- [*config 802.11a*](#)
- [*config 802.11b*](#)
- [*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 database*](#)
- [*config dhcp*](#)
- [*config known ap*](#)
- [*config interface*](#)
- [*config load-balancing*](#)
- [*config location add*](#)
- [*config location delete*](#)
- [*config location description*](#)
- [*config location enable/disable*](#)
- [*config location interface-mapping*](#)
- [*config macfilter*](#)
- [*config mgmtuser*](#)
- [*config mesh*](#)
- [*config mobility*](#)
- [*config msglog level*](#)
- [*config nac acl*](#)
- [*config nac add*](#)
- [*config nac delete*](#)
- [*config nac enable/disable*](#)

- [config netuser](#)
- [config network](#)
- [config port](#)
- [config pmk-cache delete](#)
- [config prompt](#)
- [config qos queue length](#)
- [config radius acct](#)
- [config radius auth](#)
- [config radius backward compatibility](#)
- [config radius callStationIdType](#)
- [config rfid auto-timeout](#)
- [config rfid status](#)
- [config rfid timeout](#)
- [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 access point status.
	acknowledged	This rogue access point has been identified and belongs to an external network.
	alert	This rogue access point has not been identified. Generates a trap upon detection of this access point.
	contain	Start containing a rogue access point.
	known	This rogue access point has been identified and is part of an internal network.
	<MAC address>	MAC address of the rogue access point.
	<num of APs>	Number of rogue access points.

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 antenna](#)
- [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 pico-cell](#)
- [config 802.11a rate](#)
- [config 802.11a txPower](#)

config 802.11a antenna

To configure the 802.11a antenna, use the config 802.11a antenna command.

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

```
>config 802.11a antenna <Cisco AP> <internal/external>
```

Syntax	config	Configure parameters.
	802.11a antenna	Antennas for 802.11a Cisco Radio.
	<Cisco AP>	Cisco 1000 Series lightweight access point name.
	<internal/external>	Configure for internal or external antennas.
Defaults	Internal.	
Examples	<pre>>config 802.11a antenna AP1 internal</pre> to set AP1 to use the 802.11a internal antennas.	
Related Commands	config 802.11a disable, config 802.11a enable, config 802.11a antMode	

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 WLAN Solution 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, make sure that you have disabled the 802.11a network using the config 802.11a disable command. When you are done changing the beacon period, remember to enable the 802.11a network using the config 802.11a enable command.

>config 802.11a beaconperiod <Time Units>

Syntax	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 AP> <global/channel #>}
```

Syntax	config 802.11a channel global <Cisco AP>	Configure parameters. Cisco Radio channel number. Global channel control. 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 802.11a 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 AP>}

Syntax	config	Configure parameters.
	802.11a	802.11a network parameters.
	enable/disable	Enables/disables 802.11a.
	network	Whole network.
	<Cisco AP>	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 <period>

Syntax	config 802.11a dtim <period>	Configure parameters. 802.11a network parameters. Delivery Traffic Indication Map. 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 WLAN Solution 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 AP>}

Syntax	config	Configure parameters.
	802.11a	802.11a network parameters.
	disable/enable	Disables/enables 802.11a.
	network	For the whole network.
	<Cisco AP>	Override the network setting for an individual <Cisco 1000 Series lightweight access point> Cisco Radio.
Defaults	Network = enabled.	
Examples	To enable the whole 802.11a network: >config 802.11a enable network	
	To enable AP1 802.11a transmissions: >config 802.11a enable AP1	
Related Commands	show sysinfo, show 802.11a, config wlan radio, config 802.11a disable, config 802.11b disable, config 802.11b enable, config 802.11b 11gSupport enable, config 802.11b 11gSupport disable	

config 802.11a pico-cell

To enable or disable the 802.11a pico-cell extensions, use the config 802.11a pico-cell command.

This command can only be used when the network is not operational.

>config 802.11a pico-cell <enable/disable>}

Syntax	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) auto- matic 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 currently 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 WLAN Solution 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 pico-cell*](#)
- [*config 802.11b preamble*](#)
- [*config 802.11b rate*](#)
- [*config 802.11b txPower*](#)

config 802.11b 11gSupport

After enabling the Cisco WLAN Solution 802.11b network using the config 802.11b enable command, enable or disable the Cisco WLAN Solution 802.11g network using the config 802.11b 11gSupport command. Note that you must use this command to enable the network after configuring other 802.11b parameters.

Note that this command only enables the Cisco WLAN Solution 802.11g network after the Cisco WLAN Solution 802.11b network is enabled using the config 802.11b enable command. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual 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 802.11b 11gSupport enable/disable <Cisco AP>	Configure parameters. 802.11b network parameters. Support for the 802.11g network. Enable or disable 802.11b/g. To override the network setting for individual Cisco 1000 Series lightweight access point Cisco Radio.
Defaults	Enabled.	
Examples	<pre> >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! </pre>	
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 AP> <internal/external>

Syntax	config	Configure parameters.
	802.11b antenna	Antennas for 802.11b/g Cisco Radio.
	<Cisco AP>	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 WLAN Solution 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, make sure that you have disabled the 802.11b/g network using the config 802.11b disable command. When you are done changing the beacon period, remember to enable the 802.11b/g network using the config 802.11b enable command.

>config 802.11b beaconperiod <Time Units>

Syntax	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 AP> <global/channel #>}
```

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

Defaults (none)

Examples

To have 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 AP>}

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 AP>	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 AP> <enable/sideA/sideB>

Syntax	config	Configure parameters.
	802.11b diversity	Diversity antennas for 802.11b/g.
	<Cisco AP>	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 lightweight access point Left port.
	sideB	Between the internal antennas and an external antenna connected to the Cisco 1000 Series lightweight access point Right port.

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, make sure that you have disabled the 802.11b/g network using the config 802.11b disable command. When you are done changing the DTIM value, remember to enable the 802.11b/g network using the config 802.11b enable command.

>config 802.11b dtim <period>

Syntax	config 802.11b dtim <period>	Configure parameters. 802.11b/g network parameters. Delivery Traffic Indication Map. 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 WLAN Solution 802.11b network. To enable the Cisco WLAN Solution 802.11g network, you MUST have the 802.11b network enabled, and then use the config 802.11b 11gSupport enable command. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual 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 AP>}

Syntax	config	Configure parameters.
	802.11b	802.11b network parameters.
	enable/disable	Enable or disable 802.11b. Allow support for 802.11g.
	network <Cisco AP>	For the whole network. 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 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 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 AP> <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) auto-matic configuration.
	<Cisco AP>	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 currently 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 WLAN Solution 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 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.
Defaults	Name	ACL name.
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 avoidance in making channel selection updates for all 802.11a Cisco 1000 Series lightweight access points, use the config advanced 802.11a channel foreign command.

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

Syntax	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 channel	Advanced 802.11a parameters. Radio Resource Management (RRM) channel selections.
	noise [enable/disable]	Non-802.11a noise. 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	<pre>>config advanced 802.11a monitor signal 120</pre> 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 AP> <value>

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

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

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	customize	Performance profile.
	Cisco AP	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 AP> <value>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile exception	Cisco 1000 Series lightweight access point profile exception
	global/<Cisco AP>	Global or Cisco 1000 Series lightweight access point specific profile.
	<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 AP>} <value>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile foreign	Foreign interference profile.
	global/<Cisco AP>	Global or Cisco 1000 Series lightweight access point specific profile.
	<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 AP> <value>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile level	Cisco 1000 Series lightweight access point profile level
	global/<Cisco AP>	Global or Cisco 1000 Series lightweight access point specific profile.
	<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 AP> <value>

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

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile throughput	Data rate threshold
	global/<Cisco AP>	Global or Cisco 1000 Series lightweight access point specific profile.
	<value>	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 AP> <value>

Syntax	config	Configure parameters.
	advanced 802.11a	Advanced 802.11a parameters.
	profile utilization	Cisco 1000 Series lightweight access point profile utilization
	global/<Cisco AP>	Global or Cisco 1000 Series lightweight access point specific profile.
	<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 [enable/disable]	Foreign interference. 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 channel	Advanced 802.11b/g parameters. Radio Resource Management (RRM) channel selections.
	noise [enable/disable]	Non-802.11b/g noise. 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	<pre>>config advanced 802.11b monitor coverage 60</pre> 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	<pre>>config advanced 802.11b monitor noise 120</pre> 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	<pre>>config advanced 802.11b monitor signal 120</pre> 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 AP> <value>

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	profile clients	Client profiles.
	global/<Cisco AP>	Global or Cisco 1000 Series lightweight access point specific profile.
	<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 AP> <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 AP>	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 AP> <on|off>
```

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
Defaults	Off	
Example:	<pre>>config advanced 802.11b profile customize on</pre> 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 AP> <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 AP>	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 AP>} <value> (0 to 100 percent)
```

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	profile foreign	Foreign interference profile.
	global/<Cisco AP>	Global or Cisco 1000 Series lightweight access point specific profile.
	<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 AP> <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 AP>	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 AP> <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 AP>	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 AP> <value>

Syntax	config	Configure parameters.
	advanced 802.11b	Advanced 802.11b/g parameters.
	profile throughput	Throughput profile.
	global/<Cisco AP>	Global or Cisco 1000 Series lightweight access point specific profile.
	<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 AP> <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 AP>	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	<pre>>config advanced client-handoff 100</pre> 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*](#)
- [*show advanced timers eap-identity-request-delay*](#)

config advanced timers ap-discovery-timeout

The Cisco 1000 Series lightweight access point discovery time-out is how often a Cisco Wireless LAN Controller attempts to discover unconnected Cisco 1000 Series lightweight access points. To configure the Cisco 1000 Series lightweight access point discovery time-out, use the config advanced timers ap-discovery-timeout command.

>config advanced timers ap-discovery-timeout <seconds>

Syntax	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.

>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 advanced timers eap-identity-request-delay

To configure the advanced EAP identity request delay in seconds, use the config advanced timers eap-identity-request-delay command.

```
>show advanced timers eap-identity-request-delay <seconds>
```

Syntax	show	Display configurations.
	advanced	Advanced parameters.
	timers eap-identity-request-delay	Advanced system timers.
	<seconds>	Number of seconds between 0 and 10.
Defaults	None.	
Examples	>show advanced timers eap-identity-request-delay 8	
Related Commands	config advanced timers auth-timeout, config advanced timers rogue-ap, show advanced timers	

CONFIG AP COMMANDS

Use the following config ap commands:

- [config ap disable](#)
- [config ap enable](#)
- [config ap get-crash-data](#)
- [config ap group-name](#)
- [config ap location](#)
- [config ap mode](#)
- [config ap name](#)
- [config ap primary-base](#)
- [config ap remote-debug](#)
- [config ap reporting-period](#)
- [config ap reset](#)
- [config ap sniff 802.11a](#)
- [config ap sniff 802.11b](#)
- [config ap stats-timer](#)
- [config ap secondary-base](#)
- [config ap tertiary-base](#)
- [config ap static-ip](#)
- [config ap wlan](#)

config ap disable

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

>config ap disable <Cisco AP>

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	disable	Disable command.
	<Cisco AP>	Name of the Cisco 1000 Series lightweight access point.
Defaults	(none)	
Examples	>config ap disable AP1	
Related Commands	config ap enable	

config ap enable

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

>config ap enable <Cisco AP>

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	enable	Enable command.
	<Cisco AP>	Name of the Cisco 1000 Series lightweight access point.
Defaults	(none)	
Examples	>config ap enable AP1	
Related Commands	config ap disable	

config ap 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 AP>

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	get-crash-data	Enable command.
	<Cisco AP>	Name of the Cisco 1000 Series lightweight access point.

Defaults (none)

Examples >config ap get-crash-data AP3

config ap group-name

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

```
>config ap group-name <groupname> <Cisco AP>
```

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	group name	Descriptive group name a.
	<Cisco AP>	Name of the Cisco 1000 Series lightweight access point.
Defaults	(none)	
Examples	>config ap group-name superusers AP01	
Related Commands	show ap summary	

config ap location

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

>config ap location "<location>" <Cisco AP>

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	location	Descriptive location.
	"<location>"	Location name (enclosed by double quotation marks).
	<Cisco AP>	Name of the Cisco 1000 Series lightweight access point.
Defaults	(none)	
Examples	>config ap location "Building 1" AP1	
Related Commands	show ap summary	

config ap mode

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

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

>config ap mode [local/reap/monitor/rogue/sniffer/bridge] <Cisco AP>

Syntax	config ap mode local/reap/monitor/ rogue/sniffer/bridge <Cisco AP>	Configure boot option. Set the Cisco 1000 Series lightweight access point for local (normal), reap (remote office), monitor (listen-only), rogue (rogue detector), sniffer (wireless sniffer) or bridge (bridge access point) mode. 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 office mode.	
	>config ap mode monitor AP02 sets the Cisco Wireless LAN Controller to communicate with AP02 in monitor (listen-only) mode.	
	>config ap mode rogue AP91 sets the AP91 in rogue access point detector mode.	
	>config ap mode sniffer AP02 sets the AP02 in wireless sniffer mode. It will capture and forward all the packets from the clients on that channel to a remote machine that runs AiroPeek (A packet analyzer for IEEE 802.11 wireless LANs). It will include information on timestamp, signal strength, packet size and so on.	
	>config ap mode bridge AP91 sets the AP91 in bridge mode. Note that the bridge mode can be set only on a Cisco 1030 remote edge lightweight access point.	
Related Commands	show ap config	

config ap name

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

>config ap name <New 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 primary-base

To set the Cisco 1000 Series lightweight access point primary Cisco Wireless LAN Controller, use the `config ap primary-base` command. The Cisco 1000 Series lightweight access point associates with this Cisco Wireless LAN Controller for all network operation and in the event of a hardware reset.

>config ap primary-base <Controller name> <Cisco AP>

Syntax	<code>config</code>	Configure parameters.
	<code>ap</code>	Cisco 1000 Series lightweight access point.
	<code>primary-base</code>	Cisco 1000 Series lightweight access point primary Cisco Wireless LAN Controller.
	<code><Controller name></code>	Name of Cisco Wireless LAN Controller.
	<code><Cisco AP></code>	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 AP>

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) <Cisco AP>	Optional command to be executed. 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 AP>

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

config ap sniff 802.11a

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

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

Before a Cisco 1000 Series lightweight access point can act as a sniffer, a remote computer that runs Airopeek must be set up so that it can receive packets sent by the Cisco 1000 Series lightweight access point. After the Airopeek installation, copy the following .dll files to the location where airopeek is installed.

- socket.dll file to the Plug-ins folder (Example: C:\Program Files\WildPackets\AiroPeek\Plugins)
- socketres.dll file to the PluginRes folder (Example: C:\Program Files\WildPackets\AiroPeek\1033\PluginRes)

```
>config ap sniff 802.11a <enable/disable><channel><Server-IPAddr><Cisco AP
name>]
```

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	sniff	Sniffer command.
	[802.11a <enable/disable>	Enable or disable the 802.11a radio
	<chan>	Sniffer Channel
	<Server-IPAddr>	The sniffer server (remote Airopeek ip address)
Defaults	<Cisco AP name>	Cisco AP name.
	(none)	
Example	>config ap sniff 80211a enable 23 11.22.44.55 AP01	
Related Commands	show ap config, config ap sniff 802.11b	

config ap sniff 802.11b

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

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

Before a Cisco 1000 Series lightweight access point can act as a sniffer, a remote computer that runs Airopeek must be set up so that it can receive packets sent by the Cisco 1000 Series lightweight access point. After the Airopeek installation, copy the following .dll files to the location where airopeek is installed.

- socket.dll file to the Plug-ins folder (Example: C:\Program Files\WildPackets\AiroPeek\Plugins)
- socketres.dll file to the PluginRes folder (Example: C:\Program Files\WildPackets\AiroPeek\1033\PluginRes)

```
>config ap sniff 802.11b <enable/disable><channel><Server-IPAddr><Cisco AP
name>
```

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	sniff	Sniffer command.
	802.11b <enable/disable>	Enable or disable the 802.11b radio
	<chan>	Sniffer Channel
	<Server-IPAddr>	The sniffer server (remote Airopeek ip address)
Defaults	<Cisco AP name>	Cisco AP name.
	(none)	
Example	<pre>>config ap sniff 80211b enable 23 11.22.44.55 AP01</pre>	
Related Commands	show ap config, config ap sniff 802.11a	

config ap stats-timer

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

>config ap stats-timer <period> <Cisco AP>

Syntax	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 AP>	Cisco 1000 Series lightweight access point name.

Defaults 0 (disabled)

Examples >config ap stats-timer 600 AP2

Related Commands config ap disable

config ap secondary-base

To set the Cisco 1000 Series lightweight access point secondary Cisco Wireless LAN Controller, use the `config ap secondary-base` command. The Cisco 1000 Series lightweight access point associates with this Cisco Wireless LAN Controller for all network operation and in the event of a hardware reset.

>config ap secondary-base <Controller name> <Cisco AP>

Syntax	<code>config</code>	Configure parameters.
	<code>ap</code>	Cisco 1000 Series lightweight access point.
	<code>primary-base</code>	Cisco 1000 Series lightweight access point secondary Cisco Wireless LAN Controller.
	<code><Controller name></code>	Name of Cisco Wireless LAN Controller.
	<code><Cisco AP></code>	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 AP>

Syntax	<code>config</code>	Configure parameters.
	<code>ap</code>	Cisco 1000 Series lightweight access point.
	<code>tertiary-base</code>	Cisco 1000 Series lightweight access point tertiary Cisco Wireless LAN Controller.
	<code><Controller name></code>	Name of Cisco Wireless LAN Controller.
	<code><Cisco AP></code>	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 AP 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 Cisco 1000 Series lightweight access point uses DHCP to get the IP address.
	<Cisco AP 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 AP>
```

Syntax	config	Configure parameters.
	ap	Cisco 1000 Series lightweight access point.
	wlan	Reset command.
	enable/disable/ add/delete	Enable or disable WLAN Override mode. 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 (WLAN ID)	802.11a or 802.11b/g radio. Optional Cisco Wireless LAN Controller ID assigned to a WLAN.
	<Cisco AP>	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 a 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 configure 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-Cisco Wireless LAN Controller ipsec
Defaults	N/A	
Examples	<pre>>config certificate generate webadmin</pre>	
	Creating a certificate may take some time. Do you wish to continue? (y/n)	
	<pre>>config certificate compatibility</pre>	
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:** Refer to [Cisco WLAN Solution Supported Country Codes](#) in the [Product Guide](#) for the most recent country codes and regulatory domains.

>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.	
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 database

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

>config database <size>

Syntax	config database <size>	Command action. A database size between 512 and 2040
Defaults	None.	
Examples	>config dhcp lease 003 Configures the dhcp lease for scope 003.	
Related Commands	show database	

config dhcp

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

>config dhcp

Syntax	<code>config dhcp</code> Command action. <code>address-pool <scope name> <start> <end></code> Configure an address range to allocate. <code>create-scope <name></code> Create a new dhcp scope. <code>default-router <scope></code> Configure the default routers. <code>delete-scope <scope name></code> Delete a dhcp scope. <code>disable <enable/disable> <scope name></code> Disable a scope. <code>dns-servers <scope name> <dns1> [dns2] [dns3]</code> Configure the name servers. <code>domain <scope name> <domain></code> Configure the DNS Domain Name. <code>enable <enable/disable> <scope name></code> Enable a scope. <code>lease <scope name> <lease seconds></code> Configure the lease time (in seconds). <code>netbios-name-server <scope name> <wubs1> [wins2] [wins2] [wins3]</code> Configure the netbios name servers. <code>network <scope name> <network> <netmask></code> Configure the network and netmask.
Defaults	None.
Examples	>config dhcp lease 003 Configures the dhcp lease for the scope 003
Related Commands	<code>show dhcp</code>

config known ap

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

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

Syntax	config	Configure parameters.
	known ap	Known Cisco 1000 Series lightweight access point.
	add/alert/delete	Command action.
	<MAC address>	MAC address of the known Cisco 1000 Series lightweight access point.
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>	Configures the management interface.
	<netmask> <gateway>	
	service-port <addr>	Configures the out-of-band service Port.
	<netmask>	
Defaults	virtual <addr>	Configures the virtual gateway interface.
	<interface-name>	Enter interface name.
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 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 location add

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

```
>config location add <location name>
```

Syntax	config	Configure parameters.
	location	Cisco 1000 Series lightweight access point location.
	add	Add a location.
	<location name>	Name of a location.

Defaults	(none)
-----------------	--------

Examples	>config location add warehouse
-----------------	--------------------------------

Related Commands	show location, config location enable/disable, config location delete, config location description, config interlace-mapping
-------------------------	--

config location delete

To delete an existing Cisco 1000 Series lightweight access point location, use the config location delete command.

```
>config location delete <location name>
```

Syntax	config	Configure parameters.
	location	Cisco 1000 Series lightweight access point location.
	delete	Delete a location.
	<location name>	Name of a location.

Defaults	(none)
-----------------	--------

Examples	>config location delete warehouse
-----------------	-----------------------------------

Related Commands	show location, config location add, config location enable/disable, config location description, config interlace-mapping
-------------------------	---

config location description

To specify a description of a Cisco 1000 Series lightweight access point location, use the config location description command.

```
>config location description <location name><description>]
```

Syntax	config	Configure parameters.
	location	Cisco 1000 Series lightweight access point location.
	description	Description of a location.
	<location name>	Name of a location.
	<description>	Description of a location.
Defaults	(none)	
Examples	>config location description warehouse bld02	
Related Commands	show location, config location add, config location delete, config location enable/disable, config interlace-mapping	

config location enable/disable

To enable or disable Cisco 1000 Series lightweight access point location-based overrides, use the config location disable/enable command.

>config location <enable/disable>

Syntax	config	Configure parameters.
	location	Cisco 1000 Series lightweight access point location.
	Enable or disable	Enable or disable location-based overrides.
Defaults	(none)	
Examples	>config location disable	
Related Commands	show location, config location add, config location delete, config location description, config interlace-mapping	

config location interface-mapping

To add or delete a new Cisco 1000 Series lightweight access point location/WLAN/interface mapping, use the config location interface-mapping command.

```
>config location interface-mapping{add/delete}><location name><wlan ID><interface name>
```

Syntax	config	Configure parameters.
	location	Cisco 1000 Series lightweight access point location.
	interface-mapping	
	{add/delete}>	Add or delete a new location/WLAN/interface mapping.
	<location name>	Name of a location.
	<wlan ID>]	Wlan ID.
	<interface name>	Interface name.
Defaults	(none)	
Examples	>config location interface-mapping add warehouse 13	
Related Commands	show location, config location add, config location delete, config location description, config location disable/enable	

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-compatible](#)
- [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 user name.
	"<description>"	Optional description, up to 32 characters, in double quotes.
Defaults	(none)	
Examples	<pre>>config macfilter description 11:11:11:11:11:11 engineer1 "MAC Filter 01"</pre>	
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	<code>config</code>	Configure parameters.
	<code>macfilter</code>	Local MAC address filter.
	<code>mac-delimiter</code>	MAC address format for RADIUS servers.
	<code><none colon hyphen single-hyphen></code>	MAC delimiter format. ("none" disables delimiters.)

Defaults	(none)
-----------------	--------

Examples	<pre>>config macfilter mac-delimiter colon</pre> To have OS send MAC address to RADIUS servers in the form aa:bb:cc:dd:ee:ff.
	<pre>>config macfilter mac-delimiter hyphen</pre> To have OS send MAC address to RADIUS servers in the form aa-bb-cc-dd-ee-ff.
	<pre>>config macfilter mac-delimiter none</pre> To have OS send MAC address to RADIUS servers in the form aabbccddeeff.

Related Commands	<code>show macfilter</code>
-------------------------	-----------------------------

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
Defaults	[description]	Short description
	(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 mesh

To set up mesh Cisco 1000 Series lightweight access point parameters, use the config mesh command.

```
>config mesh [rts11a<value>/rts11bg<value>/gcwmin<value>/gcwmax<value>/
gaifs<value>/bcwmin<value>/bcwmax<value>/baifs<value>/clientStatsPush-
Interval<value>/qdepth<value>/hwretries<value>/linkrate<value>/set/show]
```

Syntax	config	Configure parameters.
	mesh	Mesh command.
	<rts11a	802.11a RTS threshold.
	/rts11bg	802.11b/g RTS threshold.
	/gcwmin	Mesh Cisco 1000 Series lightweight access point 802.11g cw minimum.
	/gcwmax	Mesh Cisco 1000 Series lightweight access point 802.11g cw maximum.
	/gaifs	Mesh Cisco 1000 Series lightweight access point 802.11g aifs.
	/bcwmin	Mesh Cisco 1000 Series lightweight access point 802.11b cw minimum.
	/bcwmax	Mesh Cisco 1000 Series lightweight access point 802.11b cw maximum.
	/baifs	Mesh Cisco 1000 Series lightweight access point 802.11b aifs.
	/clientStatsPushInterval	Mesh Cisco 1000 Series lightweight access point client statistics push interval.
	/qdepth	Mesh Cisco 1000 Series lightweight access point qdepth.
	/hwretries	Mesh Cisco 1000 Series lightweight access point hardware retries.
	/linkrate	Mesh Cisco 1000 Series lightweight access point link rate.
	/set	Send current mesh Cisco 1000 Series lightweight access point parameters.
	/show>	Show current mesh ap parameters.

Defaults (none)

Examples

```
>config mesh show
11aRTSthreshold      : 56
11bgRTSthreshold     : 0
gcwMin    + 0
gswMax     : 0
gaifs      : 0
bcwMin     : 0
bcwMax     : 0
baifs      : 0
Qdepth     : 0
hwRetries  : 0
txRate     : 0
client stats push interval      : 0 minutes
Config not set since last change .... /linkrate/set/show>
```

Related Commands show mesh

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 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	Mobility group member.
	[add/delete]	Enable or disable 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 mobility group Cisco Wireless LAN Controllers, use the config mobility secure-mode command.

```
>config mobility secure-mode [enable/disable]
```

Syntax	config	Configure parameters.
	mobility	Mobility group member.
	secure-mode	Secure mode.
	[enable/disable]	Enable or disable mobility group message security.

Defaults	(none)
-----------------	--------

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

Related Commands	show mobility summary
-------------------------	-----------------------

config mobility statistics

To reset the mobility group statistics, use the config mobility statistics command.

>config mobility statistics reset

Syntax	config	Configure parameters.
	mobility	Mobility group.
	statistics	Mobility group statistics.
	reset	Reset the mobility group statistics.
Defaults	(none)	
Examples	>config mobility statistics reset	
Related Commands	show mobility statistics	

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	<code>config</code>	Configure parameters.
	<code>msglog level</code>	Message log message levels.
	<code>warning</code>	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	<code>show msglog</code>	

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 nac acl

To configure Network Access Control Access Control List name for a Cisco Wireless LAN Controller, use the config nac acl command.

```
>config nac acl <none/acl1-name>
```

Syntax	config	Configure.
	nac acl	Network Access Control acl.
	<none/	Clears the ACL Name.
	acl1-name>	Enter and acl name.
Defaults	(none)	
Examples	>config nac acl none	
Related Commands	show nac, config nac add, config nac delete, config nac disable/enable, show nac summary, show nac statistics	

config nac add

To add Network Access Control server index for a Cisco Wireless LAN Controller, use the config nac add command.

```
>config nac add <index><IP address><port><secret>
```

Syntax	config	Configure.
	nac	Network Access Control.
	add	Command action.
	<index>	NAC server index number.
	<IP Address>	NAC server IP address.
	<port>	NAC server port number.
Defaults	<secret>	NAC server secret.
	(none)	
Examples	>config nac add none	
Related Commands	show nac, config nac acl, config nac delete, config nac disable/enable, show nac summary, show nac statistics	

config nac delete

To delete a Network Access Control server for a Cisco Wireless LAN Controller, use the config nac delete command.

>show nac delete<index>

Syntax	config	Configure.
	nac	Network Access Control.
	delete	Command action.
	<index>	Index number for NAC server.
Defaults	(none)	
Examples	>config nac delete 23	
Related Commands	show nac, config nac acl, config nac add, config nac disable/enable, show nac summary, show nac statistics	

config nac enable/disable

To enable or disable a Network Access Control server for a Cisco Wireless LAN Controller, use the config nac enable/disable command.

```
>show nac [disable<index>/enable<index>]
```

Syntax	config	Configure.
	nac	Network Access Control.
	[disable/enable	Command action.
	<index>]	Index number for NAC server.
Defaults	(none)	
Examples	>config nac enable 1	
Related Commands	show nac, config nac acl, config nac add, config nac delete, show nac summary, show nac statistics	

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> <WLAN 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 arpunicast*](#)
- [*config network arptimeout*](#)
- [*config network fast-ssid-change*](#)
- [*config network master-base*](#)
- [*config network mgmt-via-wireless*](#)
- [*config network multicast*](#)
- [*config network otap-mode*](#)
- [*config network peer-blocking*](#)
- [*config network rf-network-name*](#)
- [*config network secureweb*](#)
- [*config network ssh*](#)
- [*config network telnet*](#)
- [*config network usertimeout*](#)
- [*config network web-auth-port*](#)
- [*config network webmode*](#)

config network ap-fallback

To enable or disable Cisco 1000 Series lightweight access point 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	Cisco 1000 Series lightweight access point 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 AppleTalk, 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 AppleTalk.
	<enable/disable>	Enable or disable.
Defaults	(None).	
Examples	>config network apple-talk enable	
Related Commands	show network	

config network arpunicast

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

>config network arpunicast <enable/disable>

Syntax	config	Configure parameters.
	network	Cisco Wireless LAN Controller network parameter.
	arpunicast	ARP unicast.
	<enable/disable>	Enable or disable.
Defaults	300 with a minimum of 10.	
Examples	>config network arpunicast 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 fast-ssid-change

To enable or disable fast SSID changing for mobile stations, use the config network fast-ssid-change command.

SSID (Service Set Identifier) is a code attached to all packets on a wireless network to identify each packet as part of that network.

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

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

>config network fast-ssid-change <enable/disable>

Syntax	config	Configure parameters.
	network	Cisco Wireless LAN Controller network parameter.
	fast-ssid-change	Modify fast ssid on mobile stations.
	<enable/disable>	Enable or Disable.
Defaults	None.	
Examples	>config network fast-ssid-change enable	
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	<code>config network master-base <enable/disable></code>	Configure parameters. Cisco Wireless LAN Controller network parameter. Master Cisco Wireless LAN Controller. Enables or disables a Cisco Wireless LAN Controller acting as a Cisco 1000 Series lightweight access point default master.
Defaults	(none)	
Examples	>config network master-base	
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	<code>config</code>	Configure parameters.
	<code>network</code>	Cisco Wireless LAN Controller network parameter.
	<code>mgmt-via-wireless</code>	Management sessions.
	<code>[enable/disable]</code>	Enable or disable.
Defaults	Disabled.	
Examples	>config network mgmt-via-wireless enable	
Related Commands	<code>show network</code>	

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-network-name

To set the RF mobility group domain name, use the config network rf-mobility-domain command.

```
>config network rf-network-name <name>
```

Syntax	config	Configure parameters.
	network	Cisco Wireless LAN Controller network parameter.
	rf-network-name	RF Network Name command.
	<name>	An ASCII string of 8 to 20 characters.
Defaults	(none)	
Examples	>config network rf-network-name travelers	
Related Commands	show network	

config network secureweb

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

```
>config network secureweb [enable/disable]
```

Syntax	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	<code>config</code>	Configure parameters.
	<code>network</code>	Network parameters.
	<code>usertimeout</code>	Timeout for sessions.
	<code><seconds></code>	Duration in seconds.

Defaults 300, minimum is 10.

Examples **>config network usertimeout 1200**

Related Commands `show network`

config network web-auth-port

To configure an additional port to be redirected for web authentication, use the config network web-auth-port command.

>config network web-auth-port <enable/disable>

Syntax	config	Configure parameters.
	network	Network parameters.
	web-auth-port	Web authorization port number between 0 and 65535.
	<enable/disable>	Duration in seconds.
Defaults	None.	
Examples	>config network web-auth-port 1200	
Related Commands	show network	

config pmk-cache delete

To delete an entry in the PMK cache from all Cisco Wireless LAN Controllers in the mobility group, use the config pmk-cache delete command.

```
>config pmk-cache delete [all/<MAC address>]
```

Syntax	config	Configure parameters.
	pmk-cache delete	PMK cach action.
	<all/MAC address>	All Cisco Wireless LAN Controllers or specific MAC address.
Defaults	None.	
Examples	>config pmk-cache delete all	
Related Commands	show pmk-cache	

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 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.
Default	[enable/disable]	Port state.
	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 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/ <length>	Level of quality of service: Background, Best Effort, 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 network*](#)
- [*config radius acct ipsec*](#)
- [*config radius acct retransmit-timeout*](#)

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	<pre>>config radius acct add 1 10.10.10.10 1813 ascii admin</pre> 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 acct network

To configure a default RADIUS server for network users, use the config radius acct network command.

```
>config radius acct network <index>
```

Syntax	config	Configure parameters.
	radius acct network	Default RADIUS accounting server.
	<index>	Priority index.
Defaults	(none)	
Examples	>config radius acct network 1	
Related Commands	show radius acct statistics	

config radius acct ipsec

To configure IPsec support for an accounting server for the Cisco Wireless LAN Controller, use the config radius acct ipsec command.

```
>config radius acct ipsec [enable<index>/disable<index>/authentication<hmac-md5/hmac-sha1/encryption<3des/aes/des>/ike<dh-group/lifetime/phase1>]
```

Syntax	config	Configure parameters.
	radius acct	RADIUS accounting server.
	ipsec	IPSec service.
	<enable/disable	Enable or disable IPsec support for an accounting server
	/authentication	Configure IPsec authentication
	/encryption	Configure IPsec encryption
	/ike>	Configures internet Key Exchange (IKE).
Defaults	(none)	
Examples	>config radius acct ipsec enable 1	
Related Commands	show radius acct statistics	

config radius acct retransmit-timeout

To change the default transmission timeout for a RADIUS accounting server for the Cisco Wireless LAN Controller, use the config radius acct retransmit-timeout command.

```
>config radius acct retransmit-timeout <server index><retransmit timeout>
```

Syntax	config	Configure parameters.
	radius acct	RADIUS accounting server.
	retransmit-timeout	Retransmission timeout.
	<server index>	Priority index.
	<retransmit timeout>	Timeout range of 2 through 30.
Defaults	(none)	
Examples	>config radius acct retransmit-timeout 5	
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 network*](#)
- [*config radius auth management*](#)
- [*config radius auth rfc3576*](#)
- [*config radius auth ipsec*](#)
- [*config radius auth retransmit-timeout*](#)

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	<pre>>config radius auth add 1 10.10.10.10 1812 ascii admin</pre> 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 auth network

To configure a default RADIUS server for network users, use the config radius auth network command.

```
>config radius acct network <index> <enable/disable>
```

Syntax	config	Configure parameters.
	radius auth network	Default RADIUS authentication server.
	<index>	Priority index.
	<enable/disable>	Enable or disable

Defaults (none)

Examples >config radius auth network 1 enable

Related Commands show radius acct statistics, config radius acct network

config radius auth management

To configure a default RADIUS server for management users, use the config radius auth management command.

```
>config radius auth management <index> <enable/disable>
```

Syntax	config	Configure parameters.
	radius auth network	Default RADIUS authentication server.
	<index>	Priority index.
	<enable/disable>	Enable or disable

Defaults	(none)
-----------------	--------

Examples	>config radius auth management 1 enable
-----------------	---

Related Commands	show radius acct statistics, config radius acct network
-------------------------	---

config radius auth rfc3576

To enable or disable RADIUS rfc3576 support for the authentication server for the Cisco Wireless LAN Controller, use the `config radius auth rfc3576` command.

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

```
>config radius auth rfc3576 <enable/disable><index>
```

Syntax	config	Configure parameters.
	radius auth rfc3576	Default RADIUS authentication server.
	rfc3576	RFC3576 support.
	<index>	Priority index.
	<enable/disable>	Enable or disable
Defaults	(none)	
Examples	>config radius auth rfc3576 enable 2	
Related Commands	show radius auth statistics, show radius summary, show radius rfc3576	

config radius auth ipsec

To configure IPsec support for an authentication server for the Cisco Wireless LAN Controller, use the config radius auth ipsec command.

```
>config radius auth ipsec [enable<index>/disable<index>/authentication<hmac-md5/hmac-sha1/encryption<3des/aes/des>/ike<dh-group/lifetime/phase1>]
```

Syntax	config	Configure parameters.
	radius auth	RADIUS authentication server.
	ipsec	IPSec service.
	<enable/disable	Enable or disable IPsec support for an authentication server
	/authentication	Configure IPsec authentication
	/encryption	Configure IPsec encryption
	/ike>	Configures internet Key Exchange (IKE).
Defaults	(none)	
Examples	>config radius auth ipsec enable 1	
Related Commands	show radius acct statistics	

config radius auth retransmit-timeout

To change the default transmission timeout for a RADIUS authentication server for the Cisco Wireless LAN Controller, use the config radius auth retransmit-timeout command.

```
>config radius auth retransmit-timeout <server index><retransmit timeout>
```

Syntax	config	Configure parameters.
	radius auth	RADIUS authentication server.
	retransmit-timeout	Retransmission timeout.
	<server index>	Priority index.
	<retransmit timeout>	Timeout range of 2 through 30.
Defaults	(none)	
Examples	>config radius auth retransmit-timeout 5	
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	RADIUS authentication server.
	compatibility	
	[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 callStationIdType command. This command uses the selected calling station ID for communications with RADIUS servers and other applications.

```
>config radius callStationIdType {ipAddr/macAddr/ap-macAddr}
```

Syntax	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 rfid auto-timeout

To configure the automatic timeout of RFID tags, use the config rfid auto-timeout command.

>show rfid auto-timeout <disable/enable>

Syntax	config	Configure.
	rfid	RFID configuration.
	[auto-timeout	
	<disable/enable>	Enable or disable automatic timeout.
Defaults	(none)	
Examples	>show rfid auto-timeout enable	
Related Commands	show rfid summary, config rfid status, config rfid timeout.	

config rfid status

To enable or disable RFID tag data collection, use the config rfid status command.

>show rfid status <enable/disable>

Syntax	show	Display configurations.
	rfid	RFID configuration.
	status<enable/disable>	Enable or disable rfid tag collection status.
Defaults	(none)	
Examples	>show rfid status enable	
Related Commands	show rfid summary, config rfid auto-timeout, config rfid timeout.	

config rfid timeout

To configure the static RFID tag data timeout, use the config rfid timeout command.

>show rfid timeout <seconds>

Syntax	show	Display configurations.
	rfid	RFID configuration.
	timeout <seconds>	Specify rfid timeout in seconds between 60 and 7200 seconds.
Defaults	(none)	
Examples	>show rfid timeout 60	
Related Commands	show rfid summary, config rfid statistics.	

config rogue ap

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

```
>config rogue ap <acknowledged/alert/contain/known> <MAC address> <num of APs>
```

Syntax	config	Configure parameters.
	rogue ap	Rogue access point status.
	acknowledged	This rogue access point has been identified and belongs to an external network.
	alert	This rogue access point has not been identified. Generates a trap upon detecting this access point.
	contain	Start containing a rogue access point.
	known	This rogue access point has been identified and is part of an internal network.
	<MAC address>	MAC address of the rogue access point.
	<num of APs>	Number of rogue access points.
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 ad hoc rogue access point (IBSS), use the config rogue adhoc command.

```
>config rogue adhoc <acknowledged/alert/contain> <MAC address> <num of APs>
```

Syntax	config	Configure parameters.
	rogue adhoc	Ad hoc rogue access point.
	acknowledged	This rogue access point has been identified and belongs to an external network.
	alert	This rogue access point has not been identified. Generates a trap upon detection of this access point.
	contain	Start containing an ad hoc rogue access point.
	<MAC address>	MAC address of the ad hoc rogue access point.
	<num of APs>	Number of rogue access points.
Defaults	(none)	
Example	>config rogue adhoc acknowledged 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 detecting this access point.
	contain	Start containing a rogue access point.
	<MAC address>	MAC address of the rogue access point.
	<num of APs>	Number of rogue access points.
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/	Connection speed.
	19200/38400/57600/ 115200]	

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 WLAN Solution_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> <encryptkey>
```

Syntax	config	Configure parameters.
	snmp	SNMP parameters.
	v3user	Version 3 SNMP.
	<username>	New user name.
	[rw/ro]	Read/write or read/only user privileges.
	[none/hmacmd5/hmacsha]	Authentication protocol.
	[none/des]	Encryption protocol.
	<authkey>	Authentication key, if enabled.
	<encryptkey>	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:** When the a Cisco 4400 Series Wireless LAN Controller is configured for port redundancy, spanning tree protocol must be disabled for all ports on the Cisco 4400 Series Wireless LAN Controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 Series Wireless LAN Controller.

Note that you must disable Cisco Wireless LAN Controller STP using the config spanningtree switch mode command, select STP mode for all Ethernet ports using this command, and then enable Cisco Wireless LAN Controller STP using the config spanningtree switch mode command. This procedure allows the Cisco Wireless LAN Controller to most efficiently set up STP, detect logical network loops, place redundant ports on standby, and build a network with the most efficient pathways.

>config spanningtree port mode [off/802.1d/fast] [<port>/all]

Syntax	config spanningtree port mode [off/802.1d/fast] [<port>/all]	Configure parameters. Spanning Tree Protocol. Cisco Wireless LAN Controller Ethernet port. STP mode. STP off/802.1D/fast. 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.

► **Note:** When the a Cisco 4400 Series Wireless LAN Controller is configured for port redundancy, spanning tree protocol must be disabled for all ports on the Cisco 4400 Series Wireless LAN Controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 Series Wireless LAN Controller.

>config spanningtree port pathcost [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.

▶ **Note:** When the a Cisco 4400 Series Wireless LAN Controller is configured for port redundancy, spanning tree protocol must be disabled for all ports on the Cisco 4400 Series Wireless LAN Controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 Series Wireless LAN Controller.

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

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

► **Note:** When the a Cisco 4400 Series Wireless LAN Controller is configured for port redundancy, spanning tree protocol must be disabled for all ports on the Cisco 4400 Series Wireless LAN Controller. Spanning tree protocol can remain enabled on the switch connected to the Cisco 4400 Series Wireless LAN Controller.

>config spanningtree switch bridgepriority [0-65535]

Syntax	<pre> config spanningtree switch bridgepriority [0-65535] </pre>	Configure parameters. Spanning Tree Protocol. Cisco Wireless LAN Controller. Bridge ID. 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 spanningtree switch forwarddelay [4-30]	Configure parameters. Spanning Tree Protocol. Cisco Wireless LAN Controller. Forward delay setting. 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 [6-40]	Forward delay setting. 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	<pre>>config spanningtree switch mode enable</pre> 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 <manual/ntp/timezone>

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	Disables or enables daylight savings time for the system.
	<disable/enable> <hours> [minutes]	
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-disassociate/802.11-deauthenticate/  
802.11-authfail/802.11-assocfail>[enable/disable]
```

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	client	DOT11 traps flag.
	802.11-disassociate/ 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. Modify the state of the parameter.
	[enable/disable]	
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 access point detection traps, use the config trapflags rogueap command.

>config trapflags rogueap [enable/disable]

Syntax	config	Configure parameters.
	trapflags	Trap parameters.
	rogueap	Rogue access point 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 lightweight access point interface.
	antenna>	Enable sending trap when RF manager automatically changes antenna for the Cisco 1000 Series lightweight 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 <User Name>]
```

Syntax	config watchlist	Command action.
	add	Add a watchlist entry.
	mac <MAC addr>	MAC address of new entry.
	username <User Name>	User name.
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 <User Name>]
```

Syntax	config watchlist	Command action.
	delete	Delete a watchlist entry.
	mac <MAC addr>	MAC address of new entry.
	username <User Name>	User name.
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

Use the following config wlan commands. Note that the Standalone

- [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 IPv6Support](#)
- [config wlan mac-filtering](#)
- [config wlan qos](#)
- [config wlan radio](#)
- [config wlan radius_server](#)
- [config wlan security](#)
- [config wlan timeout](#)
- [config wlan vlan](#)
- [config wlan wmm](#)
- [config wlan 802.11e](#)

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 WLAN Solution 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>
```

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.
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> <seconds>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	exclusionlist	Exclusion List.
	<WLAN id>	WLAN identifier between 1 and 16.
	<seconds>	Timeout in seconds.
Defaults	Not enabled	
Examples	<pre>>config wlan exclusionlist 16 2</pre>	
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>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	create	Add a WLAN.
	<WLAN id>	WLAN identifier between 1 and 16.
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>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	delete	Remove a WLAN.
	<WLAN id>	WLAN identifier between 1 and 16.
Defaults	(none)	
Examples	>config wlan delete 16	
Related Commands	show wlan, show wlan summary	

config wlan dhcp_server

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

```
>config wlan dhcp_server <WLAN id> <ipaddr>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	dhcp_server	Configure internal DHCP server.
	<WLAN id>	WLAN identifier between 1 and 16.
	<ipaddr>	IP Address of the internal DHCP server (this parameter is required).

Defaults (none)

Examples >config wlan dhcp_server 16 10.10.2.1

Related Commands show wlan

config wlan disable

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

```
>config wlan disable <WLAN id>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	disable	Change state of WLAN.
	<WLAN id>	WLAN identifier between 1 and 16.
Defaults	(none)	
Examples	>config wlan disable 16	
Related Commands	show wlan	

config wlan enable

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

```
>config wlan enable <WLAN id>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	enable	Change state of WLAN.
	<WLAN id>	WLAN identifier between 1 and 16.
Defaults	(none)	
Examples	>config wlan enable 16	
Related Commands	show wlan	

config wlan interface

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

```
>config wlan interface <WLAN id> <interface-name>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	interface	Change state of WLAN.
	<WLAN id>	WLAN identifier between 1 and 16.
	<interface-name>	Existing interface name.

Defaults (none)

Examples >config wlan interface 16 VLAN901

Related Commands show wlan

config wlan IPv6Support

To configure IPv6 support on a wireless LAN, use the config wlan IPv6Support command.

>config wlan IPv6support [<enable/disable><WLAN id>]

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	IPv6support	IP version 6 support.
	<enable/disable>	Enable or disable support.
	<WLAN id>	WLAN identifier between 1 and 16.
Defaults	(none)	
Examples	>config wlan IPv6support enable 6	
Related Commands	show wlan	

config wlan mac-filtering

To change the state of MAC filtering on a wireless LAN, use the config wlan mac-filtering command.

>config wlan mac-filtering [enable/disable] <WLAN id>

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.

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> [bronze/silver/gold/platinum]
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	qos	Quality of service.
	<WLAN id>	WLAN identifier between 1 and 16.
	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	
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.
Defaults	all	802.11a/b/g supported, when 802.11a, 802.11b and 802.11g support are enabled.
	(none)	
Examples	>config wlan radio 1 all	
Related Commands	config 802.11a enable, config 802.11a disable, config 802.11b enable, config 802.11b disable, config 802.11b 11gSupport enable, config 802.11b 11gSupport disable, show wlan	

config wlan radius_server

To configure a WLAN's radius servers, use the config wlan radius_server command.

```
>config wlan radius_server [auth/acct][add/delete]<WLAN id> <IP addr>all]
[<port>]
```

Syntax	config wlan radius-server [auth/acct] [add/delete] <WLAN id> [<IP addr>/all [<port>]	Configure parameters. Wireless LAN parameters. RADIUS servers. Authentication or accounting server. Add or delete a server. WLAN identifier between 1 and 16. IP address of specific server or all. Port number of the configured RADIUS server port number.
Defaults	(none)	
Examples	>config wlan radius_server 1 auth all 16	
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 wwm

To configure WWM (WME), use the config wlan wme command.

```
>config wlan wwm <allow/disable/require> <WLAN id>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	wwm	Configure WWM.
	<allow/	Allows WME on the WLAN.
	disable/	Disables WWM on the WLAN.
	require>	Requires WWM enabled clients on the WLAN.
Defaults	<WLAN id>	WLAN identifier between 1 and 16.
	(none)	
Examples	>config wlan wwm allow 1 SSID01	
Related Commands	show trapflags	

config wlan 802.11e

To configure 802.11e support on a WLAN, use the config wlan 802.11e command.

802.11e provides Quality of Service (QoS) support for LAN applications, which are critical for delay sensitive applications such as Voice over Wireless IP (VoWIP).

802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability and is especially well suited for use in networks that include multimedia capability.

>config wlan 802.11e <allow/disable/require> <WLAN id>

Syntax	config wlan 802.11e <allow/ disable/ require> <WLAN id>	Configure parameters. Wireless LAN parameters. Configure 802.11e. Allows 802.11e support on the WLAN. Select this option if you are unsure of any multimedia applications use. Disables 802.11e support on the WLAN. Select this option if you do not need to support any multimedia applications. Requires 802.11e support enabled clients on the WLAN. Select this option if multimedia applications need to be supported. WLAN identifier between 1 and 16.
Defaults	(none)	
Examples	>config wlan 802.11e allow 1 SSID01	
Related Commands	show trapflags	

CONFIG WLAN SECURITY COMMANDS

Use the following wlan security commands.

- [config wlan security 802.1X](#)
- [config wlan security cranite](#)
- [config wlan security fortress](#)
- [config wlan security ipsec authentication](#)
- [config wlan security ipsec config](#)
- [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 ipsec ike contivity](#)
- [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 encryption](#)
- [config wlan security web](#)
- [config wlan security wpa1](#)
- [config wlan security wpa2](#)

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>

Syntax	config wlan security 802.1X enable/disable/ encryption <WLAN id>	Configure parameters. Wireless LAN parameters. Security policy. 802.1X security. Change state command. Sets the static WEP keys and indexes. WLAN identifier between 1 and 16.
Defaults	(none)	
Examples	>config wlan security 802.1X enable 16	
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>
```

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.

Defaults (none)

Examples >config wlan security cranite enable 16

Related Commands show wlan

config wlan security fortress

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

```
>config wlan security fortress [enable/disable] <WLAN id>
```

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.

Defaults (none)

Examples >config wlan security fortress enable 16

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>

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.
Defaults	N/A	
Examples	>config wlan security IPSec enable 16	
Related Commands	show wlan	

config wlan security ipsec authentication

To modify the IPSec security authentication protocol used on the wireless LAN, use the config wlan security ipsec authentication command.

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>
```

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.

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>
```

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.
Defaults	N/A	
Examples	>config wlan security ipsec encryption aes 1	
Related Commands	show wlan	

config wlan security ipsec config

To configure the propriety IKE CFG-Mode parameters used on the wireless LAN, use the config wlan security ipsec config command.

IKE (Internet Key Exchange protocol) is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how the data should be protected. IKE keeps track of connections by assigning a bundle of Security Associations (SAs), to each connection.

```
>config wlan security ipsec config [qotd <ip-addr>] <WLAN id>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	ipsec	IPSec security.
	config	Configure ipsec parameter.
	[qotd	Quote-of-the-day server
	<ip-addr>]	IP address for cfg-mode
Defaults	<WLAN id>	WLAN identifier between 1 and 16.
	N/A	
Examples	>config wlan security ipsec config 44.55.66.77 1	
Related Commands	show wlan	

config wlan security ipsec ike authentication

To modify the IPSec ike authentication protocol used on the wireless LAN, use the config wlan security ipsec ike authentication command.

```
>config wlan security ipsec ike authentication <certificates/pre-share-key/
xauth-psk> <WLAN id> <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.
	<key>	Key required for pre-share and xauth-psk.
Defaults	N/A	
Examples	<pre>>config wlan security ipsec ike authentication certificates 16 <key></pre>	
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> <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.
Defaults	<group-id>	Group 1, 2 or 5
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> <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.
Defaults	<seconds>	Timeout in seconds
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>
```

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.
Defaults	N/A	
Examples	>config wlan security ipsec ike phase1 aggressive 16	
Related Commands	show wlan	

config wlan security ipsec ike contivity

To modify Nortel's Contivity VPN client support on the wireless LAN, use the config wlan security ipsec ike contivity command.

```
>config wlan security ipsec ike contivity [enable/disable] <WLAN id>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	ipsec	IPSec security.
	ike	IKE protocol.
	contivity	Contivity command.
	[enable/disable]	Enable or Disable.
	<WLAN id>	WLAN identifier between 1 and 16.
Defaults	N/A	
Examples	>config wlan security ipsec ike contivity enable 14	
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>
```

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.
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 l2tp [authentication/enable/disable/encryption/ike]
<WLAN id> [gateway]
```

Syntax	config wlan security l2tp authentication/ enable/disable encryption/ ike <WLAN id>	Configure parameters. Wireless LAN parameters. Security policy. L2tp. IPSec authentication transform (hmac-md5 or hmac-sha-1). Modify l2tp status. IPSec configuration transform (3des, aes or des). Internal Key Exchange (authentication, DH-Group, lifetime or phase1). 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.
Defaults	<WLAN id>	WLAN identifier between 1 and 16.
	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 wlan security static-wep-key encryption <WLAN id> [40/104/128] hex/ascii <key> <key-index>	Configure parameters. Wireless LAN parameters. Security policy. Static WEP key authentication. Encryption setting. WLAN identifier between 1 and 16. Encryption level. Key format Hex or ASCII key 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> <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.
	<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 wpa1

To change the status of WiFi Protected Access authentication, use the config wlan security wpa1 command.

```
>config wlan security wpa1 [enable/disable/pre-shared-key] <WLAN id>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	security	Security policy.
	wpa1	WiFi Protected Access authentication.
	enable/disable	Modify status.
	/pre-shared-key	WPA Pre-shared key mode (WPA-PSK). When Enabled, you can choose to enable a pre-shared key with or without an eight- to 63-character RSN Passphrase.
	<WLAN id>	WLAN identifier between 1 and 16.
Defaults	N/A	
Examples	>config wlan security wpa1 enable 1	
Related Commands	show wlan	

config wlan security wpa2

To change the status of WPA authentication, use the config wlan security wpa2 command.

```
>config wlan security wpa2 [enable/disable<pre-shared-key><tkip><wpa-compat>]
<WLAN id>
```

Syntax	config wlan security wpa2 <pre-shared-key> <tkip> <wpa-compat> enable/disable <WLAN id>	Configure parameters. Wireless LAN parameters. Security policy. WPA authentication. WPA2 Pre-Shared key mode. When Enabled, you can choose to enable a pre-shared key with or without an eight- to 63-character RSN Passphrase. WPA2 TKIP mode. WPA compatibility mode. Modify status. WLAN identifier between 1 and 16.
Defaults	N/A	
Examples	>config wlan security wpa2 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> <seconds>
```

Syntax	config	Configure parameters.
	wlan	Wireless LAN parameters.
	timeout	Client timeout.
	<WLAN id>	WLAN identifier between 1 and 16.
	<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> [<VLAN id/untagged> [<IP Address> <Netmask>
<Gateway>]/default]
```

Syntax	config wlan vlan <WLAN id> default <VLAN id/untagged> <IP Address> <Netmask> <Gateway> Configure parameters. Wireless LAN parameters. Virtual LAN. WLAN identifier between 1 and 16. Use the network port configuration VLAN ID or untagged If untagged, enter the IP Address, netmask and gateway
Defaults	N/A
Examples	>config wlan vlan 1 untagged default
Related Commands	show wlan wps client-exclusion ip-theft <enable/disable> Wireless protection system. Client Exclusion Internet Protocol theft or re-use. Enable or disable the client exclusion.
Defaults	N/A
Examples	>config wps client-exclusion ip-theft enable
Related Commands	config wps client-exclusion 802.11-assoc, config wps client-exclusion 802.11-auth, config wps client-exclusion 802.1x-auth, config wps client-exclusion nac, config wps client-exclusion web-auth, show wps summary config wps client-exclusion 802.11-assoc, config wps client-exclusion 802.11-auth, config wps client-exclusion 802.1x-auth, config wps client-exclusion nac, config wps client-exclusion ip-theft, show wps summary

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 AP>
```

Syntax	clear	Clear.
	ap-config	Cisco 1000 Series lightweight access point configuration.
	<Cisco AP>	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 config	Clear. 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 stats mobility	Clear. Statistics counters. 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 stats switch	Clear. Statistics counters. 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	<pre>>clear redirect-url</pre> 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 transfer	Clear. 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 traplog	Clear. 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	<pre>>clear ext-webauth-url</pre> URL cleared.	
Related Commands	clear transfer, clear download datatype, clear download filename, clear download mode, clear download path, clear download serverip, clear download start, clear upload filename, clear upload mode, clear upload path, clear upload serverip, clear upload start	

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/webadmindcert/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.
	webadmindcert	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 a 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 tftpPktMaxTimeout 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 a 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 a Cisco Wireless LAN Controller.
	filename <filename>	Enter filename up to 31 alphanumeric characters.

Defaults	N/A
-----------------	-----

Examples	<pre>>transfer upload filename build603</pre>
-----------------	--

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 a 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 a 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 a 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 upload start	Move a file. Download start operation for a Cisco Wireless LAN Controller.
Defaults	N/A	
Examples	<pre> >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 </pre>	
Related Commands	clear transfer, transfer download datatype, transfer download filename, transfer download mode, transfer download path, transfer download serverip, transfer download start, transfer upload datatype, transfer upload filename, transfer upload mode, transfer upload path, transfer upload serverip	

Troubleshooting

Use the debug commands to manage system debugging.



CAUTION: Debug commands are reserved for use only under direction of Cisco personnel. Please do not use these commands without direction from Cisco-certified staff.



Notes: