



## WLAN Commands

---

- [clear ipv6 neighbor-binding](#), on page 7
- [config 802.11 dtpc](#), on page 8
- [config advanced hotspot](#), on page 9
- [config auto-configure voice](#), on page 10
- [config client ccx clear-reports](#), on page 13
- [config client ccx clear-results](#), on page 14
- [config client ccx default-gw-ping](#), on page 15
- [config client ccx dhcp-test](#), on page 16
- [config client ccx dns-ping](#), on page 17
- [config client ccx dns-resolve](#), on page 18
- [config client ccx get-client-capability](#), on page 19
- [config client ccx get-manufacturer-info](#), on page 20
- [config client ccx get-operating-parameters](#), on page 21
- [config client ccx get-profiles](#), on page 22
- [config client ccx log-request](#), on page 23
- [config client ccx send-message](#), on page 25
- [config client ccx stats-request](#), on page 29
- [config client ccx test-abort](#), on page 30
- [config client ccx test-association](#), on page 31
- [config client ccx test-dot1x](#), on page 32
- [config client ccx test-profile](#), on page 33
- [config client deauthenticate](#), on page 34
- [config ipv6 disable](#), on page 35
- [config ipv6 enable](#), on page 36
- [config ipv6 neighbor-binding](#), on page 37
- [config ipv6 na-mcast-fwd](#), on page 39
- [config ipv6 ns-mcast-fwd](#), on page 40
- [config ipv6 ra-guard](#), on page 41
- [config remote-lan](#), on page 42
- [config remote-lan aaa-override](#), on page 43
- [config remote-lan acl](#), on page 44
- [config remote-lan create](#), on page 45
- [config remote-lan custom-web](#), on page 46

- [config remote-lan delete](#), on page 48
- [config remote-lan dhcp\\_server](#), on page 49
- [config remote-lan exclusionlist](#), on page 50
- [config remote-lan interface](#), on page 51
- [config remote-lan ldap](#), on page 52
- [config remote-lan mac-filtering](#), on page 53
- [config remote-lan max-associated-clients](#), on page 54
- [config remote-lan radius\\_server](#), on page 55
- [config remote-lan security](#), on page 57
- [config remote-lan session-timeout](#), on page 58
- [config remote-lan webauth-exclude](#), on page 59
- [config rf-profile band-select](#), on page 60
- [config rf-profile client-trap-threshold](#), on page 62
- [config rf-profile create](#), on page 63
- [config rf-profile fra client-aware](#), on page 64
- [config rf-profile data-rates](#), on page 65
- [config rf-profile delete](#), on page 66
- [config rf-profile description](#), on page 67
- [config rf-profile load-balancing](#), on page 68
- [config rf-profile max-clients](#), on page 69
- [config rf-profile multicast data-rate](#), on page 70
- [config rf-profile out-of-box](#), on page 71
- [config rf-profile tx-power-control-thresh-v1](#), on page 72
- [config rf-profile tx-power-control-thresh-v2](#), on page 73
- [config rf-profile tx-power-max](#), on page 74
- [config rf-profile tx-power-min](#), on page 75
- [config watchlist add](#), on page 76
- [config watchlist delete](#), on page 77
- [config watchlist disable](#), on page 78
- [config watchlist enable](#), on page 79
- [config wlan](#), on page 80
- [config wlan 7920-support](#), on page 81
- [config wlan 802.11e](#), on page 82
- [config wlan aaa-override](#), on page 83
- [config wlan acl](#), on page 84
- [config wlan assisted-roaming](#), on page 85
- [config wlan avc](#), on page 86
- [config wlan apgroup](#), on page 87
- [config wlan band-select allow](#), on page 94
- [config wlan broadcast-ssid](#), on page 95
- [config wlan call-snoop](#), on page 96
- [config wlan chd](#), on page 97
- [config wlan ccx aironet-ie](#), on page 98
- [config wlan channel-scan defer-priority](#), on page 99
- [config wlan channel-scan defer-time](#), on page 100
- [config wlan custom-web](#), on page 101

- [config wlan dhcp\\_server](#), on page 103
- [config wlan diag-channel](#), on page 104
- [config wlan dtim](#), on page 105
- [config wlan exclusionlist](#), on page 106
- [config wlan flow](#), on page 107
- [config wlan flexconnect ap-auth](#), on page 108
- [config wlan flexconnect learn-ipaddr](#), on page 109
- [config wlan flexconnect local-switching](#), on page 110
- [config wlan flexconnect vlan-central-switching](#), on page 112
- [config wlan hotspot](#), on page 113
- [config wlan hotspot dot11u](#), on page 114
- [config wlan hotspot dot11u 3gpp-info](#), on page 115
- [config wlan hotspot dot11u auth-type](#), on page 116
- [config wlan hotspot dot11u disable](#), on page 117
- [config wlan hotspot dot11u domain](#), on page 118
- [config wlan hotspot dot11u enable](#), on page 119
- [config wlan hotspot dot11u hessid](#), on page 120
- [config wlan hotspot dot11u ipaddr-type](#), on page 121
- [config wlan hotspot dot11u nai-realm](#), on page 122
- [config wlan hotspot dot11u network-type](#), on page 125
- [config wlan hotspot dot11u roam-oi](#), on page 126
- [config wlan hotspot hs2](#), on page 127
- [config wlan hotspot msap](#), on page 130
- [config wlan interface](#), on page 131
- [config wlan ipv6 acl](#), on page 132
- [config wlan kts-cac](#), on page 133
- [config wlan layer2 acl](#), on page 134
- [config wlan learn-ipaddr-cswlan](#), on page 135
- [config wlan ldap](#), on page 136
- [config wlan load-balance](#), on page 137
- [config wlan mac-filtering](#), on page 138
- [config wlan max-associated-clients](#), on page 139
- [config wlan max-radio-clients](#), on page 140
- [config wlan mdns](#), on page 141
- [config wlan media-stream](#), on page 142
- [config wlan mfp](#), on page 143
- [config wlan mobility foreign-map](#), on page 144
- [config wlan multicast buffer](#), on page 145
- [config wlan multicast interface](#), on page 146
- [config wlan nac](#), on page 147
- [config wlan override-rate-limit](#), on page 148
- [config wlan passive-client](#), on page 150
- [config wlan peer-blocking](#), on page 151
- [config wlan pmipv6 default-realm](#), on page 152
- [config wlan pmipv6 mobility-type](#), on page 153
- [config wlan pmipv6 profile\\_name](#), on page 154

- [config wlan policy](#), on page 155
- [config wlan profiling](#), on page 156
- [config wlan qos](#), on page 157
- [config wlan radio](#), on page 158
- [config wlan radius\\_server acct](#), on page 159
- [config wlan radius\\_server acct interim-update](#), on page 160
- [config wlan radius\\_server auth](#), on page 161
- [config wlan radius\\_server acct interim-update](#), on page 162
- [config wlan radius\\_server overwrite-interface](#), on page 163
- [config wlan roamed-voice-client re-anchor](#), on page 164
- [config wlan security 802.1X](#), on page 165
- [config wlan security ckip](#), on page 167
- [config wlan security cond-web-redirect](#), on page 168
- [config wlan security eap-passthru](#), on page 169
- [config wlan security ft](#), on page 170
- [config wlan security ft over-the-ds](#), on page 171
- [config wlan security IPsec disable](#), on page 172
- [config wlan security IPsec enable](#), on page 173
- [config wlan security IPsec authentication](#), on page 174
- [config wlan security IPsec encryption](#), on page 175
- [config wlan security IPsec config](#), on page 176
- [config wlan security IPsec ike authentication](#), on page 177
- [config wlan security IPsec ike dh-group](#), on page 178
- [config wlan security IPsec ike lifetime](#), on page 179
- [config wlan security IPsec ike phase1](#), on page 180
- [config wlan security IPsec ike contivity](#), on page 181
- [config wlan security passthru](#), on page 182
- [config wlan security pmf](#), on page 183
- [config wlan security splash-page-web-redirect](#), on page 185
- [config wlan security static-wep-key authentication](#), on page 186
- [config wlan security static-wep-key disable](#), on page 187
- [config wlan security static-wep-key enable](#), on page 188
- [config wlan security static-wep-key encryption](#), on page 189
- [config wlan security tkip](#), on page 190
- [config wlan security web-auth](#), on page 191
- [config wlan security web-passthrough acl](#), on page 193
- [config wlan security web-passthrough disable](#), on page 194
- [config wlan security web-passthrough email-input](#), on page 195
- [config wlan security web-passthrough enable](#), on page 196
- [config wlan security wpa akm 802.1x](#), on page 197
- [config wlan security wpa akm cckm](#), on page 198
- [config wlan security wpa akm ft](#), on page 199
- [config wlan security wpa akm pmf](#), on page 200
- [config wlan security wpa akm psk](#), on page 201
- [config wlan security wpa disable](#), on page 202
- [config wlan security wpa enable](#), on page 203

- [config wlan security wpa ciphers](#), on page 204
- [config wlan security wpa gtk-random](#), on page 205
- [config wlan security wpa wpa1 disable](#), on page 206
- [config wlan security wpa wpa1 enable](#), on page 207
- [config wlan security wpa wpa2 disable](#), on page 208
- [config wlan security wpa wpa2 enable](#), on page 209
- [config wlan security wpa wpa2 cache](#), on page 210
- [config wlan security wpa wpa2 cache sticky](#), on page 211
- [config wlan security wpa wpa2 ciphers](#), on page 212
- [config wlan sip-cac disassoc-client](#), on page 213
- [config wlan sip-cac send-486busy](#), on page 214
- [config wlan static-ip tunneling](#), on page 215
- [config wlan session-timeout](#), on page 216
- [config wlan uapsd compliant client enable](#), on page 217
- [config wlan uapsd compliant-client disable](#), on page 218
- [config wlan user-idle-threshold](#), on page 219
- [config wlan usertimeout](#), on page 220
- [config wlan webauth-exclude](#), on page 221
- [config wlan wifidirect](#), on page 222
- [config wlan wmm](#), on page 223
- [config Commands](#), on page 224
- [debug 11v all](#), on page 225
- [debug 11v detail](#), on page 226
- [debug 11v error](#), on page 227
- [debug 11w-pmf](#), on page 228
- [debug call-control](#), on page 229
- [debug ccxdiag](#), on page 230
- [debug ccxrm](#), on page 231
- [debug ccxs69](#), on page 232
- [debug client](#), on page 233
- [debug dhcp](#), on page 234
- [debug dhcp service-port](#), on page 235
- [debug ft](#), on page 236
- [debug hotspot](#), on page 237
- [debug ipv6](#), on page 238
- [debug profiling](#), on page 239
- [debug wcp](#), on page 240
- [show advanced hotspot](#), on page 241
- [show avc statistics wlan](#), on page 242
- [show call-control ap](#), on page 244
- [show call-control client](#), on page 248
- [show client ccx client-capability](#), on page 249
- [show client ccx frame-data](#), on page 250
- [show client ccx last-response-status](#), on page 251
- [show client ccx last-test-status](#), on page 252
- [show client ccx log-response](#), on page 253

- [show client ccx manufacturer-info](#), on page 254
- [show client ccx operating-parameters](#), on page 255
- [show client ccx profiles](#), on page 256
- [show client ccx results](#), on page 258
- [show client ccx rm](#), on page 259
- [show client ccx stats-report](#), on page 261
- [show client detail](#), on page 262
- [show client location-calibration summary](#), on page 264
- [show client probing](#), on page 265
- [show client roam-history](#), on page 266
- [show client summary](#), on page 267
- [show client wlan](#), on page 269
- [show dhcp](#), on page 270
- [show dhcp proxy](#), on page 271
- [show dhcp timeout](#), on page 272
- [show guest-lan](#), on page 273
- [show ipv6 acl](#), on page 274
- [show ipv6 neighbor-binding](#), on page 275
- [show ipv6 ra-guard](#), on page 279
- [show macfilter](#), on page 280
- [show pmk-cache](#), on page 281
- [show remote-lan](#), on page 282
- [show rf-profile summary](#), on page 284
- [show rf-profile details](#), on page 285
- [show wlan](#), on page 287
- [test pmk-cache delete](#), on page 292

## clear ipv6 neighbor-binding

To clear the IPv6 neighbor binding table entries or counters, use the **clear ipv6 neighbor-binding** command.

```
clear ipv6 neighbor-binding { table { mac mac_address | vlan vlan_id | port port | ipv6 ipv6-address
| all } | counters }
```

Syntax Description		
	<b>table</b>	Clears the IPv6 neighbor binding table.
	<b>mac</b>	Clears the neighbor binding table entries for a MAC address.
	<i>mac_address</i>	MAC address of the client.
	<b>vlan</b>	Clears the neighbor binding table entries for a VLAN.
	<i>vlan_id</i>	VLAN identifier.
	<b>port</b>	Clears the neighbor binding table entries for a port.
	<i>port</i>	Port number.
	<b>ipv6</b>	Clears the neighbor binding table entries for an IPv6 address.
	<i>ipv6_address</i>	IPv6 address of the client.
	<b>all</b>	Clears the entire neighbor binding table.
	<b>counters</b>	Clears IPv6 neighbor binding counters.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the IPv6 neighbor binding table entries for a VLAN:

```
(Cisco Controller) >clear ipv6 neighbor-binding table vlan 1
```

## config 802.11 dtpc

To enable or disable the Dynamic Transmit Power Control (DTPC) setting for an 802.11 network, use the **config 802.11 dtpc** command.

**config 802.11** { a | b } **dtpc** { enable | disable }

Syntax Description		
	<b>a</b>	Specifies the 802.11a network.
	<b>b</b>	Specifies the 802.11b/g network.
	<b>enable</b>	Enables the support for this command.
	<b>disable</b>	Disables the support for this command.

**Command Default** The default DTPC setting for an 802.11 network is enabled.

### Command History

#### Release Modification

**7.6** This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable DTPC for an 802.11a network:

```
(Cisco Controller) > config 802.11a dtpc disable
```



## config advanced hotspot

To configure advanced hotspot configurations, use the **config advanced hotspot** command.

```
config advanced hotspot { anqp-4way { disable | enable | threshold value } | cmbk-delay value | garp { disable | enable } | gas-limit { disable | enable } }
```

Syntax	Description
<b>anqp-4way</b>	Enables, disables, or, configures the Access Network Query Protocol (ANQP) four way fragment threshold.
<b>disable</b>	Disables the ANQP four way message.
<b>enable</b>	Enables the ANQP four way message.
<b>threshold</b>	Configures the ANQP fourway fragment threshold.
<i>value</i>	ANQP four way fragment threshold value in bytes. The range is from 10 to 1500. The default value is 1500.
<b>cmbk-delay</b>	Configures the ANQP comeback delay in Time Units (TUs).
<i>value</i>	ANQP comeback delay in Time Units (TUs). 1 TU is defined by 802.11 as 1024 usec. The range is from 1 milliseconds to 30 seconds.
<b>garp</b>	Disables or enables the Gratuitous ARP (GARP) forwarding to wireless network.
<b>disable</b>	Disables the Gratuitous ARP (GARP) forwarding to wireless network.
<b>enable</b>	Enables the Gratuitous ARP (GARP) forwarding to wireless network.
<b>gas-limit</b>	Limits the number of Generic Advertisement Service (GAS) request action frames sent to the switch by an access point in a given interval.
<b>disable</b>	Disables the GAS request action frame limit on access points.
<b>enable</b>	Enables the GAS request action frame limit on access points.

Command Default
None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the ANQP four way fragment threshold value:

```
(Cisco Controller) >config advanced hotspot anqp-4way threshold 200
```

## config auto-configure voice

To auto-configure voice deployment in WLANs, use the **config auto-configure voice** command.

**config auto-configure voice cisco** *wlan\_id* **radio** {**802.11a** | **802.11b** | **all**}

### Syntax Description

<b>cisco</b>	Auto-configure WLAN for voice deployment of Cisco end points.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512 (inclusive).
<b>radio</b>	Auto-configures voice deployment for a radio in a WLAN.
<b>802.11a</b>	Auto-configures voice deployment for 802.11a in a WLAN.
<b>802.11b</b>	Auto-configures voice deployment for 802.11b in a WLAN.
<b>all</b>	Auto-configures voice deployment for all radios in a WLAN.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

When you configure this command, all WLANs and radios are automatically disabled. After the completion of the configuration, the previous state of the WLANs and radios is restored.

The following example shows how to auto-configure voice deployment for all radios in a WLAN:

```
(Cisco Controller) >config auto-configure voice cisco 2 radio all
Warning! This command will automatically disable all WLAN's and Radio's.
It will be reverted to the previous state once configuration is complete.
Are you sure you want to continue? (y/N)y
```

```
Auto-Configuring these commands in WLAN for Voice..
wlan qos 2 platinum
- Success
wlan call-snoop enable 2
- Success
wlan wmm allow 2
- Success
wlan session-timeout 2 86400
- Success
wlan peer-blocking disable 2
- Success
wlan security tkip hold-down 0 2
- Success
wlan exclusionlist 2 disable
- Success
wlan mac-filtering disable 2
- Success
wlan dtim 802.11a 2 2
- Success
wlan dtim 802.11b 2 2
- Success
```

```

wlan ccx aironetIeSupport enabled 2
- Success
wlan channel-scan defer-priority 4 enable 2
- Success
wlan channel-scan defer-priority 5 enable 2
- Success
wlan channel-scan defer-priority 6 enable 2
- Success
wlan channel-scan defer-time 100 2
- Success
wlan load-balance allow disable 2
- Success
wlan mfp client enable 2
- Success
wlan security wpa akm cckm enable 2
- Success
wlan security wpa akm cckm timestamp-tolerance 5000 2
- Success
wlan band-select allow disable 2
- Success
*****

```

Auto-Configuring these commands for Voice - Radio 802.11a.

```

advanced 802.11a edca-parameter optimized-voice
- Success
802.11a cac voice acm enable
- Success
802.11a cac voice max-bandwidth 75
- Success
802.11a cac voice roam-bandwidth 6
- Success
802.11a cac voice cac-method load-based
- Success
802.11a cac voice sip disable
- Success
802.11a tsm enable
- Success
802.11a exp-bwreq enable
- Success
802.11a txPower global auto
- Success
802.11a channel global auto
- Success
advanced 802.11a channel dca interval 24
- Success
advanced 802.11a channel dca anchor-time 0
- Success
qos protocol-type platinum dot1p
- Success
qos dot1p-tag platinum 6
- Success
qos priority platinum voice voice besteffort
- Success
802.11a beacon period 100
- Success
802.11a dtpc enable
- Success
802.11a Coverage Voice RSSI Threshold -70
- Success
802.11a txPower global min 11
- Success
advanced eap eapol-key-timeout 250
- Success

```

```

    advanced 802.11a voice-mac-optimization disable
    - Success
802.11h channelswitch enable 1
    - Success
Note: Data rate configurations are not changed.
It should be changed based on the recommended values after analysis.
*****

```

Auto-Configuring these commands for Voice - Radio 802.11b.

```

    advanced 802.11b edca-parameter optimized-voice
    - Success
802.11b cac voice acm enable
    - Success
802.11b cac voice max-bandwidth 75
    - Success
802.11b cac voice roam-bandwidth 6
    - Success
802.11b cac voice cac-method load-based
    - Success
802.11b cac voice sip disable
    - Success
802.11b tsm enable
    - Success
802.11b exp-bwreq enable
    - Success
802.11b txPower global auto
    - Success
802.11b channel global auto - Success
advanced 802.11b channel dca interval 24
    - Success
advanced 802.11b channel dca anchor-time 0
    - Success
802.11b beacon period 100
    - Success
802.11b dtpc enable
    - Success
802.11b Coverage Voice RSSI Threshold -70
    - Success
802.11b preamble short
    - Success
advanced 802.11a voice-mac-optimization disable
    - Success
Note: Data rate configurations are not changed.
It should be changed based on the recommended values after analysis.

```

## config client ccx clear-reports

To clear the client reporting information, use the **config client ccx clear-reports** command.

**config client ccx clear-reports** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the reporting information of the client MAC address 00:1f:ca:cf:b6:60:

```
(Cisco Controller) >config client ccx clear-reports 00:1f:ca:cf:b6:60
```

## config client ccx clear-results

To clear the test results on the controller, use the **config client ccx clear-results** command.

**config client ccx clear-results** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the test results of the client MAC address 00:1f:ca:cf:b6:60:

```
(Cisco Controller) >config client ccx clear-results 00:1f:ca:cf:b6:60
```

## config client ccx default-gw-ping

To send a request to the client to perform the default gateway ping test, use the **config client ccx default-gw-ping** command.

**config client ccx default-gw-ping** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	This test does not require the client to use the diagnostic channel.	

The following example shows how to send a request to the client00:0b:85:02:0d:20 to perform the default gateway ping test:

```
(Cisco Controller) >config client ccx default-gw-ping 00:0b:85:02:0d:20
```

## config client ccx dhcp-test

To send a request to the client to perform the DHCP test, use the **config client ccx dhcp-test** command.

**config client ccx dhcp-test** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	This test does not require the client to use the diagnostic channel.	

The following example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the DHCP test:

```
(Cisco Controller) >config client ccx dhcp-test 00:E0:77:31:A3:55
```



## config client ccx dns-ping

To send a request to the client to perform the Domain Name System (DNS) server IP address ping test, use the **config client ccx dns-ping** command.

**config client ccx dns-ping** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	This test does not require the client to use the diagnostic channel.	

The following example shows how to send a request to a client to perform the DNS server IP address ping test:

```
(Cisco Controller) >config client ccx dns-ping 00:E0:77:31:A3:55
```

## config client ccx dns-resolve

To send a request to the client to perform the Domain Name System (DNS) resolution test to the specified hostname, use the **config client ccx dns-resolve** command.

**config client ccx dns-resolve** *client\_mac\_address* *host\_name*

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

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** This test does not require the client to use the diagnostic channel.

The following example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the DNS name resolution test to the specified hostname:

```
(Cisco Controller) >config client ccx dns-resolve 00:E0:77:31:A3:55 host_name
```

## config client ccx get-client-capability

To send a request to the client to send its capability information, use the **config client ccx get-client-capability** command.

**config client ccx get-client-capability** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client 172.19.28.40 to send its capability information:

```
(Cisco Controller) >config client ccx get-client-capability 172.19.28.40
```

## config client ccx get-manufacturer-info

To send a request to the client to send the manufacturer's information, use the **config client ccx get-manufacturer-info** command.

**config client ccx get-manufacturer-info** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client 172.19.28.40 to send the manufacturer's information:

```
(Cisco Controller) >config client ccx get-manufacturer-info 172.19.28.40
```

## config client ccx get-operating-parameters

To send a request to the client to send its current operating parameters, use the **config client ccx get-operating-parameters** command.

**config client ccx get-operating-parameters** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client 172.19.28.40 to send its current operating parameters:

```
(Cisco Controller) >config client ccx get-operating-parameters 172.19.28.40
```

## config client ccx get-profiles

To send a request to the client to send its profiles, use the **config client ccx get-profiles** command.

**config client ccx get-profiles** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client 172.19.28.40 to send its profile details:

```
(Cisco Controller) >config client ccx get-profiles 172.19.28.40
```

## config client ccx log-request

To configure a Cisco client eXtension (CCX) log request for a specified client device, use the **config client ccx log-request** command.

**config client ccx log-request** {roam | rsna | syslog} *client\_mac\_address*

Syntax Description	roam	(Optional) Specifies the request to specify the client CCX roaming log.
	<b>rsna</b>	(Optional) Specifies the request to specify the client CCX RSNA log.
	<b>syslog</b>	(Optional) Specifies the request to specify the client CCX system log.
	<i>client_mac_address</i>	MAC address of the client.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the request to specify the client CCS system log:

```
(Cisco Controller) >config client ccx log-request syslog 00:40:96:a8:f7:98
Tue Oct 05 13:05:21 2006
SysLog Response LogID=1: Status=Successful
Event Timestamp=121212121212
Client SysLog = 'This is a test syslog 2'
Event Timestamp=121212121212
Client SysLog = 'This is a test syslog 1'
Tue Oct 05 13:04:04 2006
SysLog Request LogID=1
```

The following example shows how to specify the client CCX roaming log:

```
(Cisco Controller) >config client ccx log-request roam 00:40:96:a8:f7:98
Thu Jun 22 11:55:14 2006
Roaming Response LogID=20: Status=Successful
Event Timestamp=121212121212
Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
Transition Time=100(ms)
Transition Reason: Unspecified Transition Result: Success
Thu Jun 22 11:55:04 2006
Roaming Request LogID=20
Thu Jun 22 11:54:54 2006
Roaming Response LogID=19: Status=Successful
Event Timestamp=121212121212
Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
Transition Time=100(ms)
Transition Reason: Unspecified Transition Result: Success
Thu Jun 22 11:54:33 2006 Roaming Request LogID=19
```

The following example shows how to specify the client CCX RSNA log:

```
(Cisco Controller) >config client ccx log-request rsna 00:40:96:a8:f7:98
Tue Oct 05 11:06:48 2006
RSNA Response LogID=2: Status=Successful
Event Timestamp=242424242424
Target BSSID=00:0b:85:23:26:70
RSNA Version=1
Group Cipher Suite=00-x0f-ac-01
Pairwise Cipher Suite Count = 2
Pairwise Cipher Suite 0 = 00-0f-ac-02
Pairwise Cipher Suite 1 = 00-0f-ac-04
AKM Suite Count = 2
KM Suite 0 = 00-0f-ac-01
KM Suite 1 = 00-0f-ac-02
SN Capability = 0x1
PMKID Count = 2
PMKID 0 = 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
PMKID 1 = 0a 0b 0c 0d 0e 0f 17 18 19 20 1a 1b 1c 1d 1e 1f
802.11i Auth Type: EAP_FAST
RSNA Result: Success
```



## config client ccx send-message

To send a message to the client, use the **config client ccx send-message** command.

**config client ccx send-message** *client\_mac\_address* *message\_id*

---

**Syntax Description**

*client\_mac\_address*

MAC address of the client.

---

---

*message\_id*

---

Message type that involves one of the following:

- 1—The SSID is invalid.
  - 2—The network settings are invalid.
  - 3—There is a WLAN credibility mismatch.
  - 4—The user credentials are incorrect.
  - 5—Please call support.
  - 6—The problem is resolved.
  - 7—The problem has not been resolved.
  - 8—Please try again later.
  - 9—Please correct the indicated problem.
  - 10—Troubleshooting is refused by the network.
  - 11—Retrieving client reports.
  - 12—Retrieving client logs.
  - 13—Retrieval complete.
  - 14—Beginning association test.
  - 15—Beginning DHCP test.
  - 16—Beginning network connectivity test.
  - 17—Beginning DNS ping test.
  - 18—Beginning name resolution test.
  - 19—Beginning 802.1X authentication test.
  - 20—Redirecting client to a specific profile.
  - 21—Test complete.
  - 22—Test passed.
  - 23—Test failed.
  - 24—Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.
  - 25—Log retrieval refused by the client.
  - 26—Client report retrieval refused by the client.
  - 27—Test request refused by the client.
  - 28—Invalid network (IP) setting.
  - 29—There is a known outage or problem with the network.
-

- 30—Scheduled maintenance period.

(continued on next page)

---

*message\_type (cont.)*

- 31—The WLAN security method is not correct.
  - 32—The WLAN encryption method is not correct.
  - 33—The WLAN authentication method is not correct.
- 

---

**Command Default**

None

---

**Command History**

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to send a message to the client MAC address 172.19.28.40 with the message user-action-required:

```
(Cisco Controller) >config client ccx send-message 172.19.28.40 user-action-required
```

## config client ccx stats-request

To send a request for statistics, use the **config client ccx stats-request** command.

**config client ccx stats-request** *measurement\_duration* {**dot11** | **security**} *client\_mac\_address*

Syntax Description		
<i>measurement_duration</i>	Measurement duration in seconds.	
<b>dot11</b>	(Optional) Specifies dot11 counters.	
<b>security</b>	(Optional) Specifies security counters.	
<i>client_mac_address</i>	MAC address of the client.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify dot11 counter settings:

```
(Cisco Controller) >config client ccx stats-request 1 dot11 00:40:96:a8:f7:98
Measurement duration = 1
dot11TransmittedFragmentCount          = 1
dot11MulticastTransmittedFrameCount    = 2
dot11FailedCount                        = 3
dot11RetryCount                         = 4
dot11MultipleRetryCount                 = 5
dot11FrameDuplicateCount                = 6
dot11RTSSuccessCount                   = 7
dot11RTSFailureCount                   = 8
dot11ACKFailureCount                   = 9
dot11ReceivedFragmentCount             = 10
dot11MulticastReceivedFrameCount       = 11
dot11FCSErrorCount                     = 12
dot11TransmittedFrameCount              = 13
```

## config client ccx test-abort

To send a request to the client to terminate the current test, use the **config client ccx test-abort** command.

**config client ccx test-abort** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	Only one test can be pending at a time.	

The following example shows how to send a request to a client to terminate the correct test settings:

```
(Cisco Controller) >config client ccx test-abort 11:11:11:11:11:11
```

## config client ccx test-association

To send a request to the client to perform the association test, use the **config client ccx test-association** command.

```
config client ccx test-association client_mac_address ssid bssid 802.11{a | b | g} channel
```

Syntax Description		
<i>client_mac_address</i>		MAC address of the client.
<i>ssid</i>		Network name.
<i>bssid</i>		Basic SSID.
<b>802.11a</b>		Specifies the 802.11a network.
<b>802.11b</b>		Specifies the 802.11b network.
<b>802.11g</b>		Specifies the 802.11g network.
<i>channel</i>		Channel number.

Command Default	
	None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client MAC address 00:0E:77:31:A3:55 to perform the basic SSID association test:

```
(Cisco Controller) >config client ccx test-association 00:E0:77:31:A3:55 ssid bssid 802.11a
```

## config client ccx test-dot1x

To send a request to the client to perform the 802.1x test, use the **config client ccx test-dot1x** command.

**config client ccx test-dot1x** *client\_mac\_address* *profile\_id* *bssid* **802.11** { **a** | **b** | **g** } *channel*

Syntax Description		
	<i>client_mac_address</i>	MAC address of the client.
	<i>profile_id</i>	Test profile name.
	<i>bssid</i>	Basic SSID.
	<b>802.11a</b>	Specifies the 802.11a network.
	<b>802.11b</b>	Specifies the 802.11b network.
	<b>802.11g</b>	Specifies the 802.11g network.
	<i>channel</i>	Channel number.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client to perform the 802.11b test with the profile name *profile\_01*:

```
(Cisco Controller) >config client ccx test-dot1x 172.19.28.40 profile_01 bssid 802.11b
```



## config client ccx test-profile

To send a request to the client to perform the profile redirect test, use the **config client ccx test-profile** command.

**config client ccx test-profile** *client\_mac\_address* *profile\_id*

Syntax Description		
	<i>client_mac_address</i>	MAC address of the client.
	<i>profile_id</i>	Test profile name.
		<p><b>Note</b> The <i>profile_id</i> should be from one of the client profiles for which client reporting is enabled.</p>
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client to perform the profile redirect test with the profile name `profile_01`:

```
(Cisco Controller) >config client ccx test-profile 11:11:11:11:11:11 profile_01
```

## config client deauthenticate

To disconnect a client, use the **config client deauthenticate** command.

**config client deauthenticate** {*MAC* | *IPv4/v6\_address* | *user\_name*}

Syntax Description		
<i>MAC</i>		Client MAC address.
<i>IPv4/v6_address</i>		IPv4 or IPv6 address.
<i>user_name</i>		Client user name.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to deauthenticate a client using its MAC address:

```
(Cisco Controller) >config client deauthenticate 11:11:11:11:11
```

# config ipv6 disable

To disable IPv6 globally on the Cisco WLC, use the **config ipv6 disable** command .

**config ipv6 disable**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

---

---

**Usage Guidelines** When you use this command, the controller drops all IPv6 packets and the clients will not receive any IPv6 address.

The following example shows how to disable IPv6 on the controller:

```
(Cisco Controller) >config ipv6 disable
```

# config ipv6 enable

To enable IPv6 globally on the Cisco WLC, use the **config ipv6 enable** command.

## **config ipv6 enable**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to enable IPv6 on the Cisco WLC:

```
(Cisco Controller) >config ipv6 enable
```

## config ipv6 neighbor-binding

To configure the Neighbor Binding table on the Cisco wireless LAN controller, use the **config ipv6 neighbor-binding** command.

```
config ipv6 neighbor-binding {timers {down-lifetime down_time | reachable-lifetime reachable_time
| stale-lifetime stale_time } | { ra-throttle {allow at-least at_least_value} | enable | disable |
interval-option { ignore | passthrough | throttle } | max-through {no_mcast_RA | no-limit}
| throttle-period throttle_period}}
```

Syntax	Description
<b>timers</b>	Configures the neighbor binding table timeout timers.
<b>down-lifetime</b>	Configures the down lifetime.
<i>down_time</i>	Down lifetime in seconds. The range is from 0 to 86400. The default is 30 seconds.
<b>reachable-lifetime</b>	Configures the reachable lifetime.
<i>reachable_time</i>	Reachable lifetime in seconds. The range is from 0 to 86400. The default is 300 seconds.
<b>stale-lifetime</b>	Configures the stale lifetime.
<i>stale_time</i>	Stale lifetime in seconds. The range is from 0 to 86400. The default is 86400 seconds.
<b>ra-throttle</b>	Configures IPv6 RA throttling options.
<b>allow</b>	Specifies the number of multicast RAs per router per throttle period.
<i>at_least_value</i>	Number of multicast RAs from router before throttling. The range is from 0 to 32. The default is 1.
<b>enable</b>	Enables IPv6 RA throttling.
<b>disable</b>	Disables IPv6 RA throttling.
<b>interval-option</b>	Adjusts the behavior on RA with RFC3775 interval option.
<b>ignore</b>	Indicates interval option has no influence on throttling.
<b>passthrough</b>	Indicates all RAs with RFC3775 interval option will be forwarded (default).
<b>throttle</b>	Indicates all RAs with RFC3775 interval option will be throttled.
<b>max-through</b>	Specifies unthrottled multicast RAs per VLAN per throttle period.

<i>no_mcast_RA</i>	Number of multicast RAs on VLAN by which throttling is enforced. The default multicast RAs on vlan is 10.
<b>no-limit</b>	Configures no upper bound at the VLAN level.
<b>throttle-period</b>	Configures the throttle period.
<i>throttle_period</i>	Duration of the throttle period in seconds. The range is from 10 to 86400 seconds. The default is 600 seconds.

**Command Default** This command is disabled by default.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the Neighbor Binding table:

```
(Cisco Controller) >config ipv6 neighbor-binding ra-throttle enable
```

**Related Commands** **show ipv6 neighbor-binding**

## config ipv6 na-mcast-fwd

To configure the Neighbor Advertisement multicast forwarding, use the **config ipv6 na-mcast-fwd** command.

```
config ipv6 na-mcast-fwd { enable | disable }
```

<b>Syntax Description</b>	<b>enable</b>	Enables Neighbor Advertisement multicast forwarding.
	<b>disable</b>	Disables Neighbor Advertisement multicast forwarding.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.5	This command was introduced.

### Usage Guidelines

If you enable Neighbor Advertisement multicast forwarding, all the unsolicited multicast Neighbor Advertisement from wired or wireless is not forwarded to wireless.

If you disable Neighbor Advertisement multicast forwarding, IPv6 Duplicate Address Detection (DAD) of the controller is affected.

The following example shows how to configure an Neighbor Advertisement multicast forwarding:

```
(Cisco Controller) >config ipv6 na-mcast-fwd enable
```

### Related Topics

[config ipv6 ns-mcast-fwd](#), on page 40

[debug ipv6](#), on page 238

## config ipv6 ns-mcast-fwd

To configure the nonstop multicast cache miss forwarding, use the **config ipv6 ns-mcast-fwd** command.

**config ipv6 ns-mcast-fwd** { **enable** | **disable** }

<b>Syntax Description</b>	<b>enable</b>	Enables nonstop multicast forwarding on a cache miss.
	<b>disable</b>	Disables nonstop multicast forwarding on a cache miss.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an nonstop multicast forwarding:

```
(Cisco Controller) >config ipv6 ns-mcast-fwd enable
```



## config ipv6 ra-guard

To configure the filter for Router Advertisement (RA) packets that originate from a client on an AP, use the **config ipv6 ra-guard** command.

```
config ipv6 ra-guard ap {enable | disable}
```

Syntax Description	enable	Disables RA guard on an AP.
	enable	Enables RA guard on an AP.
	disable	Disables RA guard on an AP.

Command Default	None
-----------------	------

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable IPv6 RA guard:

```
(Cisco Controller) >config ipv6 ra-guard enable
```

Related Commands	show ipv6 ra-guard
------------------	--------------------

## config remote-lan

To configure a remote LAN, use the **config remote-lan** command.

**config remote-lan** { **enable** | **disable** } { *remote-lan-id* | **all** }

Syntax Description		
<b>enable</b>	Enables a remote LAN.	
<b>disable</b>	Disables a remote LAN.	
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.	
<b>all</b>	Configures all wireless LANs.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a remote LAN with ID 2:

```
(Cisco Controller) >config remote-lan enable 2
```

## config remote-lan aaa-override

To configure user policy override through AAA on a remote LAN, use the **config remote-lan aaa-override** command.

**config remote-lan aaa-override** {**enable** | **disable**} *remote-lan-id*

Syntax Description		
<b>enable</b>	Enables user policy override through AAA on a remote LAN.	
<b>disable</b>	Disables user policy override through AAA on a remote LAN.	
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable user policy override through AAA on a remote LAN where the remote LAN ID is 2:

```
(Cisco Controller) >config remote-lan aaa-override enable 2
```

## config remote-lan acl

To specify an access control list (ACL) for a remote LAN, use the **config remote-lan acl** command.

**config remote-lan acl** *remote-lan-id* *acl\_name*

<b>Syntax Description</b>	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
	<i>acl_name</i>	ACL name.
		<b>Note</b> Use the <b>show acl summary</b> command to know the ACLs available.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify ACL1 for a remote LAN whose ID is 2:

```
(Cisco Controller) >config remote-lan acl 2 ACL1
```

## config remote-lan create

To configure a new remote LAN connection, use the **config remote-lan create** command.

**config remote-lan create** *remote-lan-id* *name*

Syntax Description		
	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
	<i>name</i>	Remote LAN name. Valid values are up to 32 alphanumeric characters.

Command Default	None
-----------------	------

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a new remote LAN, MyRemoteLAN, with the LAN ID as 3:

```
(Cisco Controller) >config remote-lan create 3 MyRemoteLAN
```

## config remote-lan custom-web

To configure web authentication for a remote LAN, use the **config remote-lan custom-web** command.

```
config remote-lan custom-web {ext-webauth-url URL } | global {enable | disable} | login-page
page-name | loginfailure-page {page-name | none} | logout-page {page-name | none} |
webauth-type {internal | customized | external} } remote-lan-id
```

### Syntax Description

<b>ext-webauth-url</b>	Configures an external web authentication URL.
<i>URL</i>	Web authentication URL for the Login page.
<b>global</b>	Configures the global status for the remote LAN.
<b>enable</b>	Enables the global status for the remote LAN.
<b>disable</b>	Disables the global status for the remote LAN.
<b>login-page</b>	Configures a login page.
<i>page-name</i>	Login page name.
<b>none</b>	Configures no login page.
<b>logout-page</b>	Configures a logout page.
<b>none</b>	Configures no logout page.
<b>webauth-type</b>	Configures the web authentication type for the remote LAN.
<b>internal</b>	Displays the default login page.
<b>customized</b>	Displays a downloaded login page.
<b>external</b>	Displays a login page that is on an external server.
<i>name</i>	Remote LAN name. Valid values are up to 32 alphanumeric characters.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are from 1 to 512.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

Follow these guidelines when you use the **config remote-lan custom-web** command:

- When you configure the external Web-Auth URL, do the following:

- Ensure that Web-Auth or Web-Passthrough Security is in enabled state. To enable Web-Auth, use the **config remote-lan security web-auth enable** command. To enable Web-Passthrough, use the **config remote-lan security web-passthrough enable** command.
- Ensure that the global status of the remote LAN is in disabled state. To enable the global status of the remote LAN, use the **config remote-lan custom-web global disable** command.
- Ensure that the remote LAN is in disabled state. To disable a remote LAN, use the **config remote-lan disable** command.
- When you configure the Web-Auth type for the remote LAN, do the following:
  - When you configure a customized login page, ensure that you have a login page configured. To configure a login page, use the **config remote-lan custom-web login-page** command.
  - When you configure an external login page, ensure that you have configured preauthentication ACL for external web authentication to function.

The following example shows how to configure an external web authentication URL for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web ext-webauth-url  
http://www.AuthorizationURL.com/ 3
```

The following example shows how to enable the global status of a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web global enable 3
```

The following example shows how to configure the login page for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web login-page custompage1 3
```

The following example shows how to configure a web authentication type with the default login page for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web webauth-type internal 3
```

# config remote-lan delete

To delete a remote LAN connection, use the **config remote-lan delete** command.

**config remote-lan delete** *remote-lan-id*

<b>Syntax Description</b>	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan delete 3
```



## config remote-lan dhcp\_server

To configure a dynamic host configuration protocol (DHCP) server for a remote LAN, use the **config remote-lan dhcp\_server** command.

```
config remote-lan dhcp_server remote-lan-id ip_address
```

Syntax Description	remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
	ip_addr	IPv4 address of the override DHCP server.

**Command Default** 0.0.0.0 is set as the default interface value.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports only IPv4 address format.

The following example shows how to configure a DHCP server for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan dhcp_server 3 209.165.200.225
```

**Related Commands** show remote-lan

## config remote-lan exclusionlist

To configure the exclusion list timeout on a remote LAN, use the **config remote-lan exclusionlist** command.

**config remote-lan exclusionlist** *remote-lan-id* {*seconds* | **disabled** | **enabled**}

Syntax Description		
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.	
<i>seconds</i>	Exclusion list timeout in seconds. A value of 0 requires an administrator override.	
<b>disabled</b>	Disables exclusion listing.	
<b>enabled</b>	Enables exclusion listing.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the exclusion list timeout to 20 seconds on a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan exclusionlist 3 20
```

## config remote-lan interface

To configure an interface for a remote LAN, use the **config remote-lan interface** command.

**config remote-lan interface** *remote-lan-id* *interface\_name*

<b>Syntax Description</b>	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
	<i>interface_name</i>	Interface name. <b>Note</b> Interface name should not be in upper case characters.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an interface myinterface for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan interface 3 myinterface
```

## config remote-lan ldap

To configure a remote LAN's LDAP servers, use the **config remote-lan ldap** command.

**config remote-lan ldap** {**add** | **delete**} *remote-lan-id index*

Syntax Description		
<b>add</b>	Adds a link to a configured LDAP server (maximum of three).	
<b>delete</b>	Deletes a link to a configured LDAP server.	
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.	
<i>index</i>	LDAP server index.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add an LDAP server with the index number 10 for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan ldap add 3 10
```

## config remote-lan mac-filtering

To configure MAC filtering on a remote LAN, use the **config remote-lan mac-filtering** command.

```
config remote-lan mac-filtering { enable | disable } remote-lan-id
```

Syntax Description	enable	Enables MAC filtering on a remote LAN.
	disable	Disables MAC filtering on a remote LAN.
	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
Command Default	MAC filtering on a remote LAN is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable MAC filtering on a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan mac-filtering disable 3
```

## config remote-lan max-associated-clients

To configure the maximum number of client connections on a remote LAN, use the **config remote-lan max-associated-clients** command.

**config remote-lan max-associated-clients** *remote-lan-id* *max-clients*

<b>Syntax Description</b>	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
	<i>max-clients</i>	Configures the maximum number of client connections on a remote LAN.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure 10 client connections on a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan max-associated-clients 3 10
```

## config remote-lan radius\_server

To configure the RADIUS servers on a remote LAN, use the **config remote-lan radius\_server** command.

```
config remote-lan radius_server {acct {{add | delete} server-index | {enable | disable} |
interim-update {interval | enable | disable}} | auth {{add | delete} server-index | {enable
| disable }} | overwrite-interface {enable | disable}} remote-lan-id
```

Syntax Description		
<b>acct</b>		Configures a RADIUS accounting server.
<b>add</b>		Adds a link to a configured RADIUS server.
<b>delete</b>		Deletes a link to a configured RADIUS server.
<i>remote-lan-id</i>		Remote LAN identifier. Valid values are between 1 and 512.
<i>server-index</i>		RADIUS server index.
<b>enable</b>		Enables RADIUS accounting for this remote LAN.
<b>disable</b>		Disables RADIUS accounting for this remote LAN.
<b>interim-update</b>		Enables RADIUS accounting for this remote LAN.
<i>interval</i>		Accounting interim interval. The range is from 180 to 3600 seconds.
<b>enable</b>		Enables accounting interim update.
<b>disable</b>		Disables accounting interim update.
<b>auth</b>		Configures a RADIUS authentication server.
<b>enable</b>		Enables RADIUS authentication for this remote LAN.
<b>disable</b>		Disables RADIUS authentication for this remote LAN.
<b>overwrite-interface</b>		Configures a RADIUS dynamic interface for the remote LAN.
<b>enable</b>		Enables a RADIUS dynamic interface for the remote LAN.
<b>disable</b>		Disables a RADIUS dynamic interface for the remote LAN.
<b>Command Default</b>	The interim update interval is set to 600 seconds.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable RADIUS accounting for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan radius_server acct enable 3
```



## config remote-lan security

To configure security policy for a remote LAN, use the **config remote-lan security** command.

```
config remote-lan security {{web-auth {enable | disable | acl | server-precedence} remote-lan-id
| {web-passthrough {enable | disable | acl | email-input} remote-lan-id}}
```

Syntax	Description
<b>web-auth</b>	Specifies web authentication.
<b>enable</b>	Enables the web authentication settings.
<b>disable</b>	Disables the web authentication settings.
<b>acl</b>	Configures an access control list.
<b>server-precedence</b>	Configures the authentication server precedence order for web authentication users.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<b>email-input</b>	Configures the web captive portal using an e-mail address.
<b>web-passthrough</b>	Specifies the web captive portal with no authentication required.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.4	The <b>802.1X</b> keyword was added.

The following example shows how to configure the security web authentication policy for remote LAN ID 1:

```
(Cisco Controller) >config remote-lan security web-auth enable 1
```

## config remote-lan session-timeout

To configure client session timeout, use the **config remote-lan session-timeout** command.

**config remote-lan session-timeout** *remote-lan-id* *seconds*

Syntax Description		
	<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
	<i>seconds</i>	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the client session timeout to 6000 seconds for a remote LAN with ID 1:

```
(Cisco Controller) >config remote-lan session-timeout 1 6000
```

## config remote-lan webauth-exclude

To configure web authentication exclusion on a remote LAN, use the **config remote-lan webauth-exclude** command.

**config remote-lan webauth-exclude** *remote-lan-id* {**enable** | **disable**}

Syntax Description		
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.	
<b>enable</b>	Enables web authentication exclusion on the remote LAN.	
<b>disable</b>	Disables web authentication exclusion on the remote LAN.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable web authentication exclusion on a remote LAN with ID 1:

```
(Cisco Controller) >config remote-lan webauth-exclude 1 enable
```

## config rf-profile band-select

To configure the RF profile band selection parameters, use the **config rf-profile band-select** command.

```
config rf-profile band-select {client-rssi rsssi | cycle-count cycles | cycle-threshold value | expire
{dual-band value | suppression value} | probe-response {enable | disable}} profile_name
```

Syntax Description		
<b>client-rssi</b>		Configures the client Received Signal Strength Indicator (RSSI) threshold for the RF profile.
<i>rsssi</i>		Minimum RSSI for a client to respond to a probe. The range is from -20 to -90 dBm.
<b>cycle-count</b>		Configures the probe cycle count for the RF profile. The cycle count sets the number of suppression cycles for a new client.
<i>cycles</i>		Value of the cycle count. The range is from 1 to 10.
<b>cycle-threshold</b>		Configures the time threshold for a new scanning RF Profile band select cycle period. This setting determines the time threshold during which new probe requests from a client come in a new scanning cycle.
<i>value</i>		Value of the cycle threshold for the RF profile. The range is from 1 to 1000 milliseconds.
<b>expire</b>		Configures the expiration time of clients for band select.
<b>dual-band</b>		Configures the expiration time for pruning previously known dual-band clients. After this time elapses, clients become new and are subject to probe response suppression.
<i>value</i>		Value for a dual band. The range is from 10 to 300 seconds.
<b>suppression</b>		Configures the expiration time for pruning previously known 802.11b/g clients. After this time elapses, clients become new and are subject to probe response suppression.
<i>value</i>		Value for suppression. The range is from 10 to 200 seconds.
<b>probe-response</b>		Configures the probe response for a RF profile.
<b>enable</b>		Enables probe response suppression on clients operating in the 2.4-GHz band for a RF profile.
<b>disable</b>		Disables probe response suppression on clients operating in the 2.4-GHz band for a RF profile.
<i>profile name</i>		Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

### Command Default

The default value for client RSSI is -80 dBm.

The default cycle count is 2.

The default cycle threshold is 200 milliseconds.

The default value for dual-band expiration is 60 seconds.

The default value for suppression expiration is 20 seconds.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4-GHz and moves the dual band clients to the 5-GHz spectrum. The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running. Band selection can be used only with Cisco Aironet 1040, 1140, and 1250 Series and the 3500 series access points.

The following example shows how to configure the client RSSI:

```
(Cisco Controller) >config rf-profile band-select client-rssi -70
```

## config rf-profile client-trap-threshold

To configure the threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller, use the **config rf-profile client-trap-threshold** command.

**config rf-profile client-trap-threshold** *threshold profile\_name*

<b>Syntax Description</b>	<i>threshold</i>	Threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller. The range is from 0 to 200. Traps are disabled if the threshold value is configured as zero.
	<i>profile_name</i>	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the threshold value of the number of clients that associate with an access point:

```
(Cisco Controller) >config rf-profile client-trap-threshold 150
```

## config rf-profile create

To create a RF profile, use the **config rf-profile create** command.

```
config rf-profile create { 802.11a | 802.11b/g } profile-name
```

<b>Syntax Description</b>	<b>802.11a</b>	Configures the RF profile for the 2.4GHz band.
	<b>802.11b/g</b>	Configures the RF profile for the 5GHz band.
	<i>profile-name</i>	Name of the RF profile.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to create a new RF profile:

```
(Cisco Controller) >config rf-profile create 802.11a RFtestgroup1
```

## config rf-profile fra client-aware

To configure the RF profile client-aware FRA feature, use the **config rf-profile fra client-aware** command.

```
config rf-profile fra client-aware { client-reset percent rf-profile-name | client-select percent rf-profile-name
| disable rf-profile-name | enable rf-profile-name }
```

### Syntax Description

<b>client-reset</b>	Configures the RF profile AP utilization threshold for radio to switch back to Monitor mode.
<i>percent</i>	Utilization percentage value ranges from 0 to 100. The default is 5%.
<i>rf-profile-name</i>	Name of the RF Profile.
<b>client-select</b>	Configures the RF profile utilization threshold for radio to switch to 5GHz.
<i>percent</i>	Utilization percentage value ranges from 0 to 100. The default is 50%.
<b>disable</b>	Disables the RF profile client-aware FRA feature.
<b>enable</b>	Enables the RF profile client-aware FRA feature.

### Command Default

The default percent value for client-select and client-reset is 50% and 5% respectively.

### Command History

Release	Modification
8.5	This command was introduced.

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch back from 5GHz client-serving role to Monitor mode:

```
(Cisco Controller) >config rf-profile fra client-aware client-reset 15 profile1
```

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch from Monitor mode to 5GHz client-serving role:

```
(Cisco Controller) >config rf-profile fra client-aware client-select 20 profile1
```

The following example shows how to disable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware disable profile1
```

The following example shows how to enable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware enable profile1
```



## config rf-profile data-rates

To configure the data rate on a RF profile, use the **config rf-profile data-rates** command.

```
config rf-profile data-rates {802.11a | 802.11b} {disabled | mandatory | supported} data-rate
profile-name
```

Syntax Description		
<b>802.11a</b>		Specifies 802.11a as the radio policy of the RF profile.
<b>802.11b</b>		Specifies 802.11b as the radio policy of the RF profile.
<b>disabled</b>		Disables a rate.
<b>mandatory</b>		Sets a rate to mandatory.
<b>supported</b>		Sets a rate to supported.
<i>data-rate</i>		802.11 operational rates, which are 1*, 2*, 5.5*, 6, 9, 11*, 12, 18, 24, 36, 48 and 54, where * denotes 802.11b only rates.
<i>profile-name</i>		Name of the RF profile.

### Command Default

Default data rates for RF profiles are derived from the controller system defaults, the global data rate configurations. For example, if the RF profile's radio policy is mapped to 802.11a then the global 802.11a data rates are copied into the RF profiles at the time of creation.

The data rates set with this command are negotiated between the client and the Cisco wireless LAN controller. If the data rate is set to mandatory, the client must support it in order to use the network. If a data rate is set as supported by the Cisco wireless LAN controller, any associated client that also supports that rate may communicate with the Cisco lightweight access point using that rate. It is not required that a client is able to use all the rates marked supported in order to associate.

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the 802.11b transmission of an RF profile at a mandatory rate at 12 Mbps:

```
(Cisco Controller) >config rf-profile 802.11b data-rates mandatory 12 RFGroup1
```

## config rf-profile delete

To delete a RF profile, use the **config rf-profile delete** command.

**config rf-profile delete** *profile-name*

<b>Syntax Description</b>	<i>profile-name</i>	Name of the RF profile.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a RF profile:

```
(Cisco Controller) >config rf-profile delete RFGroup1
```

## config rf-profile description

To provide a description to a RF profile, use the **config rf-profile description** command.

**config rf-profile description** *description profile-name*

<b>Syntax Description</b>	<i>description</i>	Description of the RF profile.
	<i>profile-name</i>	Name of the RF profile.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a description to a RF profile:

```
(Cisco Controller) >config rf-profile description This is a demo description RFGroup1
```

# config rf-profile load-balancing

To configure load balancing on an RF profile, use the **config rf-profile load-balancing** command.

**config rf-profile load-balancing** { **window** *clients* | **denial** *value* } *profile\_name*

## Syntax Description

<b>window</b>	Configures the client window for load balancing of an RF profile.
<i>clients</i>	<p>Client window size that limits the number of client associations with an access point. The range is from 0 to 20. The default value is 5.</p> <p>The window size is part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:</p> $\text{load-balancing window} + \text{client associations on AP with lightest load} = \text{load-balancing threshold}$ <p>Access points with more client associations than this threshold are considered busy, and clients can associate only to access points with client counts lower than the threshold. This window also helps to disassociate sticky clients.</p>
<b>denial</b>	Configures the client denial count for load balancing of an RF profile.
<i>value</i>	<p>Maximum number of association denials during load balancing. The range is from 1 to 10. The default value is 3.</p> <p>When a client tries to associate on a wireless network, it sends an association request to the access point. If the access point is overloaded and load balancing is enabled on the controller, the access point sends a denial to the association request. If there are no other access points in the range of the client, the client tries to associate the same access point again. After the maximum denial count is reached, the client is able to associate. Association attempts on an access point from any client before associating any AP is called a sequence of association. The default is 3.</p>
<i>profile_name</i>	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

## Command Default

None

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the client window size for an RF profile:

```
(Cisco Controller) >config rf-profile load-balancing window 15
```

## config rf-profile max-clients

To configure the maximum number of client connections per access point of an RF profile, use the **config rf-profile max-clients** commands.

**config rf-profile max-clients** *clients*

<b>Syntax Description</b>	<i>clients</i> Maximum number of client connections per access point of an RF profile. The range is from 1 to 200.				
<b>Command Default</b>	None				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.6</td> <td>This command was introduced in a release earlier than Release 7.6.</td> </tr> </tbody> </table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				
<b>Usage Guidelines</b>	<p>You can use this command to configure the maximum number of clients on access points that are in client dense areas, or serving high bandwidth video or mission critical voice applications.</p> <p>The following example shows how to set the maximum number of clients at 50:</p> <pre>(Cisco Controller) &gt;config rf-profile max-clients 50</pre>				

## config rf-profile multicast data-rate

To configure the minimum RF profile multicast data rate, use the **config rf-profile multicast data-rate** command.

**config rf-profile multicast data-rate** *value profile\_name*

Syntax Description	<i>value</i>	Minimum RF profile multicast data rate. The options are 6, 9, 12, 18, 24, 36, 48, 54. Enter 0 to specify that access points will dynamically adjust the data rate.
	<i>profile_name</i>	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
Command Default	The minimum RF profile multicast data rate is 0.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the multicast data rate for an RF profile:

```
(Cisco Controller) >config rf-profile multicast data-rate 24
```

## config rf-profile out-of-box

To create an out-of-box AP group consisting of newly installed access points, use the **config rf-profile out-of-box** command.

**config rf-profile out-of-box** { **enable** | **disable** }

<b>Syntax Description</b>	<p><b>enable</b> Enables the creation of an out-of-box AP group. When you enable this command, the following occurs:</p> <ul style="list-style-type: none"> <li>• Newly installed access points that are part of the default AP group will be part of the out-of-box AP group and their radios will be switched off, which eliminates any RF instability caused by the new access points.</li> <li>• All access points that do not have a group name become part of the out-of-box AP group.</li> <li>• Special RF profiles are created per 802.11 band. These RF profiles have default-settings for all the existing RF parameters and additional new configurations.</li> </ul> <p><b>disable</b> Disables the out-of-box AP group. When you disable this feature, only the subscription of new APs to the out-of-box AP group stops. All APs that are subscribed to the out-of-box AP group remain in this AP group. You can move APs to the default group or a custom AP group upon network convergence.</p>				
<b>Command Default</b>	None				
<b>Command History</b>	<table border="1"> <thead> <tr> <th data-bbox="386 1104 609 1136">Release</th> <th data-bbox="609 1104 1528 1136">Modification</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 1157 609 1188">7.6</td> <td data-bbox="609 1157 1528 1188">This command was introduced in a release earlier than Release 7.6.</td> </tr> </tbody> </table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				
<b>Usage Guidelines</b>	<p>When an out-of-box AP associates with the controller for the first time, it will be redirected to a special AP group and the RF profiles applicable to this AP Group will control the radio admin state configuration of the AP. You can move APs to the default group or a custom group upon network convergence.</p> <p>The following example shows how to enable the creation of an out-of-box AP group:</p> <pre>(Cisco Controller) &gt;config rf-profile out-of-box enable</pre>				

## config rf-profile tx-power-control-thresh-v1

To configure Transmit Power Control version1 (TPCv1) to an RF profile, use the **config rf-profile tx-power-control-thresh-v1** command.

**config rf-profile tx-power-control-thresh-v1** *tpc-threshold profile\_name*

<b>Syntax Description</b>	<i>tpc-threshold</i>	TPC threshold.
	<i>profile-name</i>	Name of the RF profile.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure TPCv1 on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v1 RFGroup1
```



## config rf-profile tx-power-control-thresh-v2

To configure Transmit Power Control version 2 (TPCv2) to an RF profile, use the **config rf-profile tx-power-control-thresh-v2** command.

```
config rf-profile tx-power-control-thresh-v2 tpc-threshold profile-name
```

<b>Syntax Description</b>	<i>tpc-threshold</i>	TPC threshold.
	<i>profile-name</i>	Name of the RF profile.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure TPCv2 on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v2 RFGroup1
```

## config rf-profile tx-power-max

To configure maximum auto-rf to an RF profile, use the **config rf-profile tx-power-max** command.

**config rf-profile** *tx-power-max profile-name*

<b>Syntax Description</b>	<i>tx-power-max</i>	Maximum auto-rf tx power.
	<i>profile-name</i>	Name of the RF profile.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure tx-power-max on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-max RFGroup1
```

## config rf-profile tx-power-min

To configure minimum auto-rf to an RF profile, use the **config rf-profile tx-power-min** command.

```
config rf-profile tx-power-min tx-power-min profile-name
```

<b>Syntax Description</b>	<i>tx-power-min</i>	Minimum auto-rf tx power.
	<i>profile-name</i>	Name of the RF profile.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure tx-power-min on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-min RFGroup1
```

## config watchlist add

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

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

<b>Syntax Description</b>	<b>mac</b> <i>MAC</i>	Specifies the MAC address of the wireless LAN.
	<b>username</b> <i>username</i>	Specifies the name of the user to watch.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a watchlist entry for the MAC address a5:6b:ac:10:01:6b:

```
(Cisco Controller) >config watchlist add mac a5:6b:ac:10:01:6b
```

## config watchlist delete

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

```
config watchlist delete { mac MAC | username username }
```

<b>Syntax Description</b>	<b>mac</b> <i>MAC</i>	Specifies the MAC address of the wireless LAN to delete from the list.
	<b>username</b> <i>username</i>	Specifies the name of the user to delete from the list.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a watchlist entry for the MAC address a5:6b:ac:10:01:6b:

```
(Cisco Controller) >config watchlist delete mac a5:6b:ac:10:01:6b
```

# config watchlist disable

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

## **config watchlist disable**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to disable the client watchlist:

```
(Cisco Controller) >config watchlist disable
```

# config watchlist enable

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

## **config watchlist enable**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to enable a watchlist entry:

```
(Cisco Controller) >config watchlist enable
```

# config wlan

To create, delete, enable, or disable a wireless LAN, use the **config wlan** command.

**config wlan** {**enable** | **disable** | **create** | **delete**} *wlan\_id* [*name* | **foreignAp** *name ssid* | **all**]

## Syntax Description

<b>enable</b>	Enables a wireless LAN.
<b>disable</b>	Disables a wireless LAN.
<b>create</b>	Creates a wireless LAN.
<b>delete</b>	Deletes a wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>name</i>	(Optional) WLAN profile name up to 32 alphanumeric characters.
<b>foreignAp</b>	(Optional) Specifies the third-party access point settings.
<i>ssid</i>	SSID (network name) up to 32 alphanumeric characters.
<b>all</b>	(Optional) Specifies all wireless LANs.

## Command Default

None

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

## Usage Guidelines

When you create a new WLAN using the **config wlan create** command, it is created in disabled mode. Leave it disabled until you have finished configuring it.

If you do not specify an SSID, the profile *name* parameter is used for both the profile name and the SSID.

If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

The following example shows how to enable wireless LAN identifier 16:

```
(Cisco Controller) >config wlan enable 16
```



## config wlan 7920-support

To configure support for phones, use the **config wlan 7920-support** command.

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

Syntax Description		
<b>ap-cac-limit</b>		Supports phones that require client-controlled Call Admission Control (CAC) that expect the Cisco vendor-specific information element (IE).
<b>client-cac-limit</b>		Supports phones that require access point-controlled CAC that expect the IEEE 802.11e Draft 6 QBSS-load.
<b>enable</b>		Enables phone support.
<b>disable</b>		Disables phone support.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.

Command Default	
	None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

The following example shows how to enable the phone support that requires client-controlled CAC with wireless LAN ID 8:

```
(Cisco Controller) >config wlan 7920-support ap-cac-limit enable 8
```

## config wlan 802.11e

To configure 802.11e support on a wireless LAN, use the **config wlan 802.11e** command.

```
config wlan 802.11e { allow | disable | require } wlan_id
```

Syntax Description		
<b>allow</b>	Allows 802.11e-enabled clients on the wireless LAN.	
<b>disable</b>	Disables 802.11e on the wireless LAN.	
<b>require</b>	Requires 802.11e-enabled clients on the wireless LAN.	
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** 802.11e provides quality of service (QoS) support for LAN applications, which are critical for delay sensitive applications such as Voice over Wireless IP (VoWIP).

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

The following example shows how to allow 802.11e on the wireless LAN with LAN ID 1:

```
(Cisco Controller) >config wlan 802.11e allow 1
```

## config wlan aaa-override

To configure a user policy override via AAA on a wireless LAN, use the **config wlan aaa-override** command.

```
config wlan aaa-override {enable | disable} {wlan_id | foreignAp}
```

Syntax Description	enable	disable	wlan_id	foreignAp
	enable	disable	wlan_id	foreignAp
	Enables a policy override.			
	Disables a policy override.			
	Wireless LAN identifier between 1 and 512.			
	Specifies third-party access points.			
Command Default	AAA is disabled.			
Command History	Release	Modification		
	7.6	This command was introduced in a release earlier than Release 7.6.		

### Usage Guidelines

When AAA override is enabled and a client has conflicting AAA and Cisco wireless LAN controller wireless LAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system will move clients from the default Cisco wireless LAN VLAN to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system will also use QoS, DSCP, 802.1p priority tag values, and ACLs provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as Identity Networking.)

If the corporate wireless LAN uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.

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

The AAA override values might come from a RADIUS server.

The following example shows how to configure user policy override via AAA on WLAN ID 1:

```
(Cisco Controller) >config wlan aaa-override enable 1
```

## config wlan acl

To configure a wireless LAN access control list (ACL), use the **config wlan acl** command.

**config wlan acl** [*acl\_name* | **none**]

Syntax Description		
<i>wlan_id</i>	Wireless LAN identifier (1 to 512).	
<i>acl_name</i>	(Optional) ACL name.	
<b>none</b>	(Optional) Clears the ACL settings for the specified wireless LAN.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a WLAN access control list with WLAN ID 1 and ACL named *office\_1*:

```
(Cisco Controller) >config wlan acl 1 office_1
```

## config wlan assisted-roaming

To configure assisted roaming on a WLAN, use the **config wlan assisted-roaming** command.

```
config wlan assisted-roaming { neighbor-list | dual-list | prediction } { enable | disable } wlan_id
```

### Syntax Description

<b>neighbor-list</b>	Configures an 802.11k neighbor list for a WLAN.
<b>dual-list</b>	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
<b>prediction</b>	Configures an assisted roaming optimization prediction for a WLAN.
<b>enable</b>	Enables the configuration on the WLAN.
<b>disable</b>	Disables the configuration on the WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512 (inclusive).

### Command Default

The 802.11k neighbor list is enabled for all WLANs.

By default, dual band list is enabled if the neighbor list feature is enabled for the WLAN.

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN, if load balancing is already enabled on the WLAN.

The following example shows how to enable an 802.11k neighbor list for a WLAN:

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```

## config wlan avc

To configure Application Visibility and Control (AVC) on a WLAN, use the **config wlan avc** command.

**config wlan avc** *wlan\_id* { **profile** *profile\_name* | **visibility** } { **enable** | **disable** }

### Syntax Description

<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
<b>profile</b>	Associates or removes an AVC profile from a WLAN.
<i>profile_name</i>	Name of the AVC profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
<b>visibility</b>	Configures application visibility on a WLAN.
<b>enable</b>	Enables application visibility on a WLAN. You can view the classification of applications based on the Network Based Application Recognition (NBAR) deep packet inspection technology.  Use the <b>show avc statistics client</b> command to view the client AVC statistics.
<b>disable</b>	Disables application visibility on a WLAN.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

You can configure only one AVC profile per WLAN and each AVC profile can have up to 32 rules. Each rule states a Mark or Drop action for an application, which allows you to configure up to 32 application actions per WLAN. You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs.

The following example shows how to associate an AVC profile with a WLAN:

```
(Cisco Controller) >config wlan avc 5 profile profile1 enable
```

## config wlan apgroup

To manage access point group VLAN features, use the **config wlan apgroup** command.

```
config wlan apgroup {add apgroup_name [description] | delete apgroup_name | description
apgroup_name description | interface-mapping {add | delete} apgroup_name wlan_id interface_name
| nac-snmp {enable | disable} apgroup_name wlan_id | nasid NAS-ID apgroup_name |
profile-mapping {add | delete} apgroup_name profile_name | wlan-radio-policy apgroup_name
wlan-id {802.11a-only | 802.11bg | 802.11g-only | all} | hotspot {venue {type apgroup_name
group_codetype_code | name apgroup_name language_codevenue_name } | operating-class {add |
delete} apgroup_name operating_class_value}}
```

### Syntax Description

<b>add</b>	Creates a new access point group (AP group).
<i>apgroup_name</i>	Access point group name.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
<b>delete</b>	Removes a wireless LAN from an AP group.
<b>description</b>	Describes an AP group.
<i>description</i>	Description of the AP group.
<b>interface-mapping</b>	(Optional) Assigns or removes a Wireless LAN from an AP group.
<i>interface_name</i>	(Optional) Interface to which you want to map an AP group.
<b>nac-snmp</b>	Configures NAC SNMP functionality on given AP group. Enables or disables Network Admission Control (NAC) out-of-band support on an access point group.
<b>enable</b>	Enables NAC out-of-band support on an AP group.
<b>disable</b>	Disables NAC out-of-band support on an AP group.
<i>NAS-ID</i>	Network Access Server identifier (NAS-ID) for the AP group. The NAS-ID is sent to the RADIUS server by the controller (as a RADIUS client) using the authentication request, which is used to classify users to different groups. You can enter up to 32 alphanumeric characters. Beginning in Release 7.4 and later releases, you can configure the NAS-ID on the interface, WLAN, or an access point group. The order of priority is AP group NAS-ID > WLAN NAS-ID > Interface NAS-ID.
<b>none</b>	Configures the controller system name as the NAS-ID.

<b>profile-mapping</b>	Configures RF profile mapping on an AP group.
<i>profile_name</i>	RF profile name for a specified AP group.
<b>wlan-radio-policy</b>	Configures WLAN radio policy on an AP group.
<b>802.11a-only</b>	Configures WLAN radio policy on an AP group.
<b>802.11bg</b>	Configures WLAN radio policy on an AP group.
<b>802.11g-only</b>	Configures WLAN radio policy on an AP group.
<b>all</b>	Configures WLAN radio policy on an AP group.
<b>hotspot</b>	Configures a HotSpot on an AP group.
<b>venue</b>	Configures venue information for an AP group.
<b>type</b>	Configures the type of venue for an AP group.
<i>group_code</i>	Venue group information for an AP group. The following options are available: <ul style="list-style-type: none"> <li>• 0 : UNSPECIFIED</li> <li>• 1 : ASSEMBLY</li> <li>• 2 : BUSINESS</li> <li>• 3 : EDUCATIONAL</li> <li>• 4 : FACTORY-INDUSTRIAL</li> <li>• 5 : INSTITUTIONAL</li> <li>• 6 : MERCANTILE</li> <li>• 7 : RESIDENTIAL</li> <li>• 8 : STORAGE</li> <li>• 9 : UTILITY-MISC</li> <li>• 10 : VEHICULAR</li> <li>• 11 : OUTDOOR</li> </ul>



---

*type\_code*

---

Venue type information for an AP group.

For venue group 1 (ASSEMBLY), the following options are available:

- 0 : UNSPECIFIED ASSEMBLY
- 1 : ARENA
- 2 : STADIUM
- 3 : PASSENGER TERMINAL
- 4 : AMPHITHEATER
- 5 : AMUSEMENT PARK
- 6 : PLACE OF WORSHIP
- 7 : CONVENTION CENTER
- 8 : LIBRARY
- 9 : MUSEUM
- 10 : RESTAURANT
- 11 : THEATER
- 12 : BAR
- 13 : COFFEE SHOP
- 14 : ZOO OR AQUARIUM
- 15 : EMERGENCY COORDINATION CENTER

For venue group 2 (BUSINESS), the following options are available:

- 0 : UNSPECIFIED BUSINESS
- 1 : DOCTOR OR DENTIST OFFICE
- 2 : BANK
- 3 : FIRE STATION
- 4 : POLICE STATION
- 6 : POST OFFICE
- 7 : PROFESSIONAL OFFICE
- 8 : RESEARCH AND DEVELOPMENT FACILITY
- 9 : ATTORNEY OFFICE

---

For venue group 3 (EDUCATIONAL), the following

options are available:

- 0 : UNSPECIFIED EDUCATIONAL
- 1 : PRIMARY SCHOOL
- 2 : SECONDARY SCHOOL
- 3 : UNIVERSITY OR COLLEGE

For venue group 4 (FACTORY-INDUSTRIAL), the following options are available:

- 0 : UNSPECIFIED FACTORY AND INDUSTRIAL
- 1 : FACTORY

For venue group 5 (INSTITUTIONAL), the following options are available:

- 0 : UNSPECIFIED INSTITUTIONAL
- 1 : HOSPITAL
- 2 : LONG-TERM CARE FACILITY
- 3 : ALCOHOL AND DRUG RE-HABILITATION CENTER
- 4 : GROUP HOME
- 5 : PRISON OR JAIL

For venue group 6 (MERCANTILE), the following options are available:

- 0 : UNSPECIFIED MERCANTILE
  - 1 : RETAIL STORE
  - 2 : GROCERY MARKET
  - 3 : AUTOMOTIVE SERVICE STATION
  - 4 : SHOPPING MALL
  - 5 : GAS STATION
-

For venue group 7 (RESIDENTIAL), the following options are available:

- 0 : UNSPECIFIED RESIDENTIAL
- 1 : PRIVATE RESIDENCE
- 2 : HOTEL OR MOTEL
- 3 : DORMITORY
- 4 : BOARDING HOUSE

For venue group 8 (STORAGE), the following options are available:

- 0 : UNSPECIFIED STORAGE

For venue group 9 (UTILITY-MISC), the following options are available:

- 0 : UNSPECIFIED UTILITY AND MISCELLANEOUS

For venue group 10 (VEHICULAR), the following options are available:

- 0 : UNSPECIFIED VEHICULAR
- 1 : AUTOMOBILE OR TRUCK
- 2 : AIRPLANE
- 3 : BUS
- 4 : FERRY
- 5 : SHIP OR BOAT
- 6 : TRAIN
- 7 : MOTOR BIKE

For venue group 11 (OUTDOOR), the following options are available:

- 0 : UNSPECIFIED OUTDOOR
  - 1 : MINI-MESH NETWORK
  - 2 : CITY PARK
  - 3 : REST AREA
  - 4 : TRAFFIC CONTROL
  - 5 : BUS STOP
  - 6 : KIOSK
-

<b>name</b>	Configures the name of venue for an AP group.
<i>language_code</i>	An ISO-639 encoded string defining the language used at the venue. This string is a three character language code. For example, you can enter ENG for English.
<i>venue_name</i>	Venue name for this AP group. This name is associated with the basic service set (BSS) and is used in cases where the SSID does not provide enough information about the venue. The venue name is case-sensitive and can be up to 252 alphanumeric characters.
<b>add</b>	Adds an operating class for an AP group.
<b>delete</b>	Deletes an operating class for an AP group.
<i>operating_class_value</i>	Operating class for an AP group. The available operating classes are 81, 83, 84, 112, 113, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127.

**Command Default** AP Group VLAN is disabled.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** An error message appears if you try to delete an access point group that is used by at least one access point. Before you can delete an AP group in controller software release 6.0, move all APs in this group to another group. The access points are not moved to the default-group access point group as in previous releases. To see the APs, enter the **show wlan apgroups** command. To move APs, enter the **config ap group-name groupname cisco\_ap** command.

The NAS-ID configured on the controller for AP group or WLAN or interface is used for authentication. The NAS-ID is not propagated across controllers.

The following example shows how to enable the NAC out-of band support on access point group 4:

```
(Cisco Controller) >config wlan apgroup nac enable apgroup 4
```

## config wlan band-select allow

To configure band selection on a WLAN, use the **config wlan band-select allow** command.

```
config wlan band-select allow {enable | disable} wlan_id
```

### Syntax Description

**enable** Enables band selection on a WLAN.

**disable** Disables band selection on a WLAN.

*wlan\_id* Wireless LAN identifier between 1 and 512.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4-GHz and moves the dual band clients to the 5-GHz spectrum. The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running. Band selection can be used only with Cisco Aironet 1040, 1140, and 1250 Series and the 3500 series access points.

The following example shows how to enable band selection on a WLAN:

```
(Cisco Controller) >config wlan band-select allow enable 6
```

## config wlan broadcast-ssid

To configure an Service Set Identifier (SSID) broadcast on a wireless LAN, use the **config wlan broadcast-ssid** command.

```
config wlan broadcast-ssid {enable | disable} wlan_id
```

Syntax Description	enable	disable	wlan_id
	enable	disable	wlan_id
	enable	disable	wlan_id
	enable	disable	wlan_id

  

Command Default	Broadcasting of SSID is disabled.
-----------------	-----------------------------------

  

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an SSID broadcast on wireless LAN ID 1:

```
(Cisco Controller) >config wlan broadcast-ssid enable 1
```

## config wlan call-snoop

To enable or disable Voice-over-IP (VoIP) snooping for a particular WLAN, use the **config wlan call-snoop** command.

**config wlan call-snoop** { **enable** | **disable** } *wlan\_id*

Syntax Description		
<b>enable</b>		Enables VoIP snooping on a wireless LAN.
<b>disable</b>		Disables VoIP snooping on a wireless LAN.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** WLAN should be with Platinum QoS and it needs to be disabled while invoking this CLI

The following example shows how to enable VoIP snooping for WLAN 3:

```
(Cisco Controller) >config wlan call-snoop 3 enable
```



## config wlan chd

To enable or disable Coverage Hole Detection (CHD) for a wireless LAN, use the **config wlan chd** command.

```
config wlan chd wlan_id {enable | disable}
```

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>enable</b>	Enables SSID broadcasts on a wireless LAN.
	<b>disable</b>	Disables SSID broadcasts on a wireless LAN.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable CHD for WLAN 3:

```
(Cisco Controller) >config wlan chd 3 enable
```

## config wlan ccx aironet-ie

To enable or disable Aironet information elements (IEs) for a WLAN, use the **config wlan ccx aironet-ie** command.

**config wlan ccx aironet-ie** { **enable** | **disable** }

<b>Syntax Description</b>	<b>enable</b>	Enables the Aironet information elements.
	<b>disable</b>	Disables the Aironet information elements.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable Aironet information elements for a WLAN:

```
(Cisco Controller) >config wlan ccx aironet-ie enable
```

## config wlan channel-scan defer-priority

To configure the controller to defer priority markings for packets that can defer off channel scanning, use the `config wlan channel-scan defer-priority` command.

```
config wlan channel-scan defer-priority priority [enable | disable] wlan_id
```

Syntax Description		
<i>priority</i>	User priority value (0 to 7).	
<b>enable</b>	(Optional) Enables packet at given priority to defer off channel scanning.	
<b>disable</b>	(Optional) Disables packet at given priority to defer off channel scanning.	
<i>wlan_id</i>	Wireless LAN identifier (1 to 512).	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

The priority value should be set to 6 on the client and on the WLAN.

The following example shows how to enable the controller to defer priority markings that can defer off channel scanning with user priority value 6 and WLAN id 30:

```
(Cisco Controller) >config wlan channel-scan defer-priority 6 enable 30
```

## config wlan channel-scan defer-time

To assign the channel scan defer time in milliseconds, use the **config wlan channel-scan defer-time** command.

**config wlan channel-scan defer-time** *msecs wlan\_id*

Syntax Description		
<i>msecs</i>		Deferral time in milliseconds (0 to 60000 milliseconds).
<i>wlan_id</i>		Wireless LAN identifier from 1 to 512.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** The time value in milliseconds should match the requirements of the equipment on your WLAN.

The following example shows how to assign the scan defer time to 40 milliseconds for WLAN with ID 50:

```
(Cisco Controller) >config wlan channel-scan defer-time 40 50
```

## config wlan custom-web

To configure the web authentication page for a WLAN, use the **config wlan custom-web** command.

```
config wlan custom-web { { ext-webauth-url ext-webauth-url wlan_id } | { global { enable | disable } }
| { login-page page-name } | { loginfailure-page { page-name | none } } | { logout-page { page-name
| none } } | { sleep-client { enable | disable } wlan_id timeout duration } | { webauth-type
{ internal | customized | external } wlan_id } }
```

Syntax Description	
<b>ext-webauth-url</b>	Configures an external web authentication URL.
<i>ext-webauth-url</i>	External web authentication URL.
<i>wlan_id</i>	WLAN identifier. Default range is from 1 to 512.
<b>global</b>	Configures the global status for a WLAN.
<b>enable</b>	Enables the global status for a WLAN.
<b>disable</b>	Disables the global status for a WLAN.
<b>login-page</b>	Configures the name of the login page for an external web authentication URL.
<i>page-name</i>	Login page name for an external web authentication URL.
<b>loginfailure-page</b>	Configures the name of the login failure page for an external web authentication URL.
<b>none</b>	Does not configure a login failure page for an external web authentication URL.
<b>logout-page</b>	Configures the name of the logout page for an external web authentication URL.
<b>sleep-client</b>	Configures the sleep client feature on the WLAN.
<b>timeout</b>	Configures the sleep client timeout on the WLAN.
<i>duration</i>	Maximum amount of time after the idle timeout, in hours, before a sleeping client is forced to reauthenticate. The range is from 1 to 720. The default is 12. When the sleep client feature is enabled, the clients need not provide the login credentials when they move from one Cisco WLC to another (if the Cisco WLCs are in the same mobility group) between the sleep and wake-up times.
<b>webauth-type</b>	Configures the type of web authentication for the WLAN.
<b>internal</b>	Displays the default login page.
<b>customized</b>	Displays a customized login page.
<b>external</b>	Displays a login page on an external web server.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure web authentication type in the WLAN.

```
Cisco Controller config wlan custom-web webauth-type external
```

## config wlan dhcp\_server

To configure the internal DHCP server for a wireless LAN, use the **config wlan dhcp\_server** command.

```
config wlan dhcp_server {wlan_id | foreignAp} ip_address [required]
```

Syntax Description		
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.
<b>foreignAp</b>		Specifies third-party access points.
<i>ip_address</i>		IP address of the internal DHCP server (this parameter is required).
<b>required</b>		(Optional) Specifies whether DHCP address assignment is required.

Command Default	None
-----------------	------

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override. If you enable the override, you can use the **show wlan** command to verify that the DHCP server has been assigned to the WLAN.

The following example shows how to configure an IP address 10.10.2.1 of the internal DHCP server for wireless LAN ID 16:

```
(Cisco Controller) >config wlan dhcp_server 16 10.10.2.1
```

## config wlan diag-channel

To enable the diagnostic channel troubleshooting on a particular WLAN, use the **config wlan diag-channel** command.

**config wlan diag-channel** [**enable** | **disable**] *wlan\_id*

Syntax Description		
<b>enable</b>	(Optional) Enables the wireless LAN diagnostic channel.	
<b>disable</b>	(Optional) Disables the wireless LAN diagnostic channel.	
<i>wlan_id</i>	Wireless LAN identifier (1 to 512).	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the wireless LAN diagnostic channel for WLAN ID 1:

```
(Cisco Controller) >config wlan diag-channel enable 1
```



## config wlan dtim

To configure a Delivery Traffic Indicator Message (DTIM) for 802.11 radio network **config wlan dtim** command.

```
config wlan dtim {802.11a | 802.11b} dtim wlan_id
```

Syntax Description	802.11a	802.11b	dtim	wlan_id
	Configures DTIM for the 802.11a radio network.	Configures DTIM for the 802.11b radio network.	Value for DTIM (between 1 to 255 inclusive).	Number of the WLAN to be configured.
<b>Command Default</b>	The default is DTIM 1.			
<b>Command History</b>	<b>Release</b>	<b>Modification</b>		
	7.6	This command was introduced in a release earlier than Release 7.6.		

The following example shows how to configure DTIM for 802.11a radio network with DTIM value 128 and WLAN ID 1:

```
(Cisco Controller) >config wlan dtim 802.11a 128 1
```

# config wlan exclusionlist

To configure the wireless LAN exclusion list, use the **config wlan exclusionlist** command.

```
config wlan exclusionlist {wlan_id [enabled | disabled | time] | foreignAp [enabled | disabled | time] }
```

Syntax Description		
<i>wlan_id</i>		Wireless LAN identifier (1 to 512).
<b>enabled</b>		(Optional) Enables the exclusion list for the specified wireless LAN or foreign access point.
<b>disabled</b>		(Optional) Disables the exclusion list for the specified wireless LAN or a foreign access point.
<i>time</i>		(Optional) Exclusion list timeout in seconds. A value of zero (0) specifies infinite time.
<b>foreignAp</b>		Specifies a third-party access point.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** This command replaces the **config wlan blacklist** command.

The following example shows how to enable the exclusion list for WLAN ID 1:

```
(Cisco Controller) >config wlan exclusionlist 1 enabled
```

## config wlan flow

To associate a NetFlow monitor with a WLAN, use the **config wlan flow** command.

```
config wlan flow wlan_id monitor monitor_name {enable | disable}
```

Syntax Description		
<i>wlan_id</i>		Wireless LAN identifier from 1 to 512 (inclusive).
<b>monitor</b>		Configures a NetFlow monitor.
<i>monitor_name</i>		Name of the NetFlow monitor. The monitor name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces for a monitor name.
<b>enable</b>		Associates a NetFlow monitor with a WLAN.
<b>disable</b>		Dissociates a NetFlow monitor from a WLAN.

Command Default	
	None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

You can use the **config flow** command to create a new NetFlow monitor.

The following example shows how to associate a NetFlow monitor with a WLAN:

```
(Cisco Controller) >config wlan flow 5 monitor monitor1 enable
```

## config wlan flexconnect ap-auth

To configure local authentication of clients associated with FlexConnect on a locally switched WLAN, use the **config wlan flexconnect ap-auth** command.

```
config wlan flexconnect ap-auth wlan_id {enable | disable}
```

Syntax Description	Parameter	Description
	<b>ap-auth</b>	Configures local authentication of clients associated with an FlexConnect on a locally switched WLAN.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>enable</b>	Enables AP authentication on a WLAN.
	<b>disable</b>	Disables AP authentication on a WLAN.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** Local switching must be enabled on the WLAN where you want to configure local authentication of clients associated with FlexConnect.

The following example shows how to enable authentication of clients associated with FlexConnect on a specified WLAN:

```
(Cisco Controller) >config wlan flexconnect ap-auth 6 enable
```

# config wlan flexconnect learn-ipaddr

To enable or disable client IP address learning for the Cisco WLAN controller, use the **config wlan flexconnect learn-ipaddr** command.

```
config wlan flexconnect learn-ipaddr wlan_id {enable | disable}
```

Syntax Description		
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>enable</b>	Enables client IPv4 address learning on a wireless LAN.
	<b>disable</b>	Disables client IPv4 address learning on a wireless LAN.

**Command Default** Disabled when the **config wlan flexconnect local-switching** command is disabled. Enabled when the **config wlan flexconnect local-switching** command is enabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports only IPv4 address format.

**Usage Guidelines** If the client is configured with Layer 2 encryption, the controller cannot learn the client IP address, and the controller will periodically drop the client. Disable this option to keep the client connection without waiting to learn the client IP address.



**Note** This command is valid only for IPv4.



**Note** The ability to disable IP address learning is not supported with FlexConnect central switching.

The following example shows how to disable client IP address learning for WLAN 6:

```
(Cisco Controller) >config wlan flexconnect learn-ipaddr disable 6
```

**Related Commands** `show wlan`

## config wlan flexconnect local-switching

To configure local switching, central DHCP, NAT-PAT, or the override DNS option on a FlexConnect WLAN, use the **config wlan flexconnect local switching** command.

```
config wlan flexconnect local-switching wlan_id {enable | disable} { {central-dhcp {enable | disable} nat-pat {enable | disable} } | {override option dns { enable | disable} } }
```

### Syntax Description

<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
<b>enable</b>	Enables local switching on a FlexConnect WLAN.
<b>disable</b>	Disables local switching on a FlexConnect WLAN.
<b>central-dhcp</b>	Configures central switching of DHCP packets on the local switching FlexConnect WLAN. When you enable this feature, the DHCP packets received from the AP are centrally switched to the controller and forwarded to the corresponding VLAN based on the AP and the SSID.
<b>enable</b>	Enables central DHCP on a FlexConnect WLAN.
<b>disable</b>	Disables central DHCP on a FlexConnect WLAN.
<b>nat-pat</b>	Configures Network Address Translation (NAT) and Port Address Translation (PAT) on the local switching FlexConnect WLAN.
<b>enable</b>	Enables NAT-PAT on the FlexConnect WLAN.
<b>disable</b>	Disables NAT-PAT on the FlexConnect WLAN.
<b>override</b>	Specifies the DHCP override options on the FlexConnect WLAN.
<b>option dns</b>	Specifies the override DNS option on the FlexConnect WLAN. When you override this option, the clients get their DNS server IP address from the AP, not from the controller.
<b>enable</b>	Enables the override DNS option on the FlexConnect WLAN.
<b>disable</b>	Disables the override DNS option on the FlexConnect WLAN.

### Command Default

This feature is disabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports only IPv4 address format.

**Usage Guidelines**

When you enable the **config wlan flexconnect local-switching** command, the **config wlan flexconnect learn-ipaddr** command is enabled by default.



**Note** This command is valid only for IPv4.



**Note** The ability to disable IP address learning is not supported with FlexConnect central switching.

The following example shows how to enable WLAN 6 for local switching and enable central DHCP and NAT-PAT:

```
(Cisco Controller) >config wlan flexconnect local-switching 6 enable central-dhcp enable nat-pat enable
```

The following example shows how to enable the override DNS option on WLAN 6:

```
(Cisco Controller) >config wlan flexconnect local-switching 6 override option dns enable
```

# config wlan flexconnect vlan-central-switching

To configure central switching on a locally switched WLAN, use the **config wlan flexconnect vlan-central-switching** command.

```
config wlan flexconnect vlan-central-switching wlan_id { enable | disable }
```

Syntax Description		
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
<b>enable</b>	Enables central switching on a locally switched wireless LAN.	
<b>disable</b>	Disables central switching on a locally switched wireless LAN.	
Command Default	Central switching is disabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** You must enable Flexconnect local switching to enable VLAN central switching. When you enable WLAN central switching, the access point bridges the traffic locally if the WLAN is configured on the local IEEE 802.1Q link. If the VLAN is not configured on the access point, the AP tunnels the traffic back to the controller and the controller bridges the traffic to the corresponding VLAN.

WLAN central switching does not support:

- FlexConnect local authentication.
- Layer 3 roaming of local switching client.

The following example shows how to enable WLAN 6 for central switching:

```
(Cisco Controller) >config wlan flexconnect vlan-central-switching 6 enable
```



# config wlan hotspot

To configure a HotSpot on a WLAN, use the **config wlan hotspot** command.

```
config wlan hotspot { clear-all wlan_id | dot11u | hs2 | msap }
```

## Syntax Description

<b>clear-all</b>	Clears the HotSpot configurations on a WLAN.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
<b>dot11u</b>	Configures an 802.11u HotSpot on a WLAN.
<b>hs2</b>	Configures HotSpot2 on a WLAN.
<b>msap</b>	Configures the Mobility Services Advertisement Protocol (MSAP) on a WLAN.

## Command Default

None

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

## Usage Guidelines

You can configure up to 32 HotSpot WLANs.

The following example shows how to configure HotSpot2 for a WLAN:

```
(Cisco Controller) >config wlan hotspot hs2 enable 2
```

## config wlan hotspot dot11u

To configure an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u** command.

```
config wlan hotspot dot11u {3gpp-info | auth-type | enable | disable | domain | hessid |
ipaddr-type | nai-realm | network-type | roam-oi}
```

Syntax	Description
<b>3gpp-info</b>	Configures 3GPP cellular network information.
<b>auth-type</b>	Configures the network authentication type.
<b>disable</b>	Disables 802.11u on the HotSpot profile.
<b>domain</b>	Configures a domain.
<b>enable</b>	Enables 802.11u on the HotSpot profile. IEEE 802.11u enables automatic WLAN offload for 802.1X devices at the HotSpot of mobile or roaming partners.
<b>hessid</b>	Configures the Homogenous Extended Service Set Identifier (HESSID). The HESSID is a 6-octet MAC address that uniquely identifies the network.
<b>ipaddr-type</b>	Configures the IPv4 address availability type.
<b>nai-realm</b>	Configures a realm for 802.11u enabled WLANs.
<b>network-type</b>	Configures the 802.11u network type and Internet access.
<b>roam-oi</b>	Configures the roaming consortium Organizational Identifier (OI) list.

**Command Default** None.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports only IPv4 address format.

The following example shows how to enable 802.11u on a HotSpot profile:

```
(Cisco Controller) >config wlan hotspot dot11u enable 6
```

## config wlan hotspot dot11u 3gpp-info

To configure 3GPP cellular network information on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u 3gpp-info** command.

```
config wlan hotspot dot11u 3gpp-info {add | delete} index country_code network_code wlan_id
```

Syntax Description	Parameter	Description
	<b>add</b>	Adds mobile cellular network information.
	<b>delete</b>	Deletes mobile cellular network information.
	<i>index</i>	Cellular index. The range is from 1 to 32.
	<i>country_code</i>	Mobile Country Code (MCC) in Binary Coded Decimal (BCD) format. The country code can be up to 3 characters. For example, the MCC for USA is 310.
	<i>network_code</i>	Mobile Network Code (MNC) in BCD format. An MNC is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator or carrier. The network code can be up to 3 characters. For example, the MNC for T-Mobile is 026.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** Number of mobile network codes supported is 32 per WLAN.

The following example shows how to configure 3GPP cellular network information on a WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u 3gpp-info add
```

## config wlan hotspot dot11u auth-type

To configure the network authentication type on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u auth-type** command.

**config wlan hotspot dot11u auth-type** *network-auth wlan\_id*

<b>Syntax Description</b>	<p><i>network-auth</i> Network authentication that you would like to configure on the WLAN. The available values are as follows:</p> <ul style="list-style-type: none"> <li>• 0—Acceptance of terms and conditions</li> <li>• 1—On-line enrollment</li> <li>• 2—HTTP/HTTPS redirection</li> <li>• 3—DNS Redirection</li> <li>• 4—Not Applicable</li> </ul>
	<p><i>wlan_id</i> Wireless LAN identifier between 1 and 512.</p>

**Command Default** None

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** The DNS redirection option is not supported in Release 7.3.

The following example shows how to configure HTTP/HTTPS redirection as the network authentication type on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u auth-type 2 1
```

## config wlan hotspot dot11u disable

To disable an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u disable** command.

**config wlan hotspot dot11u disable** *wlan\_id*

---

**Syntax Description**

*wlan\_id* Wireless LAN identifier between 1 and 512.

---

---

**Command Default**

None

---

---

**Command History**

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to disable an 802.11u HotSpot on a WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u disable 6
```

## config wlan hotspot dot11u domain

To configure a domain operating in the 802.11 access network, use the **config wlan hotspot dot11u domain** command.

**config wlan hotspot dot11u domain** { **add** *wlan\_id domain-index domain\_name* | **delete** *wlan\_id domain-index* | **modify** *wlan\_id domain-index domain\_name* }

### Syntax Description

<b>add</b>	Adds a domain.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>domain-index</i>	Domain index in the range 1 to 32.
<i>domain_name</i>	Domain name. The domain name is case sensitive and can be up to 255 alphanumeric characters.
<b>delete</b>	Deletes a domain.
<b>modify</b>	Modifies a domain.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a domain in the 802.11 access network:

```
(Cisco Controller) >config wlan hotspot dot11u domain add 6 30 domain1
```

## config wlan hotspot dot11u enable

To enable an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u enable** command.

**config wlan hotspot dot11u enable** *wlan\_id*

<b>Syntax Description</b>	<i>wlan_id</i> Wireless LAN identifier between 1 and 512.
---------------------------	---

<b>Command Default</b>	None
------------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable an 802.11u HotSpot on a WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u enable 6
```

## config wlan hotspot dot11u hessid

To configure a Homogenous Extended Service Set Identifier (HESSID) on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u hessid** command.

**config wlan hotspot dot11u hessid** *hessid wlan\_id*

<b>Syntax Description</b>	<i>hessid</i>	MAC address that can be configured as an HESSID. The HESSID is a 6-octet MAC address that uniquely identifies the network. For example, Basic Service Set Identification (BSSID) of the WLAN can be used as the HESSID.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an HESSID on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u hessid 00:21:1b:ea:36:60 6
```



## config wlan hotspot dot11u ipaddr-type

To configure the type of IP address available on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u ipaddr-type** command.

**config wlan hotspot dot11u ipaddr-type** *IPv4Type* {0 - 7} *IPv6Type* {0 - 2} *wlan\_id*

Syntax Description	
<i>IPv4Type</i>	IPv4 type address. Enter one of the following values: 0—IPv4 address not available. 1—Public IPv4 address available. 2—Port restricted IPv4 address available. 3—Single NAT enabled private IPv4 address available. 4—Double NAT enabled private IPv4 address available. 5—Port restricted IPv4 address and single NAT enabled IPv4 address available. 6—Port restricted IPv4 address and double NAT enabled IPv4 address available. 7— Availability of the IPv4 address is not known.
<i>IPv6Type</i>	IPv6 type address. Enter one of the following values: 0—IPv6 address not available. 1—IPv6 address available. 2—Availability of the IPv6 address is not known.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

**Command Default** The default values for IPv4 type address is 1.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports only IPv4 address format.

The following example shows how to configure the IP address availability type on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u ipaddr-type 6 2 6
```

**Related Commands** `show wlan`

## config wlan hotspot dot11u nai-realm

To configure realms for an 802.11u HotSpot WLANs, use the **config wlan hotspot dot11u nai-realm** command.

```
config wlan hotspot dot11u nai-realm { add | delete | modify } { auth-method wlan_id realm-index eap-index auth-index auth-method auth-parameter | eap-method wlan_id realm-index eap-index eap-method | realm-name wlan_id realm-index realm }
```

### Syntax Description

<b>add</b>	Adds a realm.
<b>delete</b>	Deletes a realm.
<b>modify</b>	Modifies a realm.
<b>auth-method</b>	Specifies the authentication method used.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
<i>realm-index</i>	Realm index. The range is from 1 to 32.
<i>eap-index</i>	EAP index. The range is from 1 to 4.
<i>auth-index</i>	Authentication index value. The range is from 1 to 10.
<i>auth-method</i>	Authentication method to be used. The range is from 1 to 4. The following options are available: <ul style="list-style-type: none"> <li>• 1—Non-EAP Inner Auth Method</li> <li>• 2—Inner Auth Type</li> <li>• 3—Credential Type</li> <li>• 4—Tunneled EAP Method Credential Type</li> </ul>
<i>auth-parameter</i>	Authentication parameter to use. This value depends on the authentication method used. See the following table for more details.
<b>eap-method</b>	Specifies the Extensible Authentication Protocol (EAP) method used.

*eap-method* EAP Method. The range is from 0 to 7. The following options are available:

- 0—Not Applicable
- 1—Lightweight Extensible Authentication Protocol (LEAP)
- 2—Protected EAP (PEAP)
- 3—EAP-Transport Layer Security (EAP-TLS)
- 4—EAP-FAST (Flexible Authentication via Secure Tunneling)
- 5—EAP for GSM Subscriber Identity Module (EAP-SIM)
- 6—EAP-Tunneled Transport Layer Security (EAP-TTLS)
- 7—EAP for UMTS Authentication and Key Agreement (EAP-AKA)

**realm-name** Specifies the name of the realm.

*realm* Name of the realm. The realm name should be RFC 4282 compliant. For example, Cisco. The realm name is case-sensitive and can be up to 255 alphanumeric characters.

#### Command Default

None

#### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

#### Usage Guidelines

This table lists the authentication parameters.

**Table 1: Authentication Parameters**

Non-EAP Inner Method(1)	Inner Authentication EAP Method Type(2)	Credential Type(3)/Tunneled EAP Credential Type(4)
0—Reserved	1—LEAP	1—SIM
1—Password authentication protocol (PAP)	2—PEAP	2—USIM
2—Challenge-Handshake Authentication Protocol (CHAP)	3—EAP-TLS	3—NFC Secure Element
3—Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)	4—EAP-FAST	4—Hardware Token
4—MSCHAPV2	5—EAP-SIM	5—Soft Token
	6—EAP-TTLS	6—Certificate
	7—EAP-AKA	7—Username/Password
		8—Reserver
		9—Anonymous
		10—Vendor Specific

The following example shows how to add the Tunneled EAP Method Credential authentication method on WLAN 4:

```
(Cisco Controller) >config wlan hotspot dot11u nai-realm add auth-method 4 10 3 5 4 6
```

## config wlan hotspot dot11u network-type

To configure the network type and internet availability on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u network-type** command.

**config wlan hotspot dot11u network-type** *wlan\_id network-type internet-access*

Syntax Description	
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
<i>network-type</i>	Network type. The available options are as follows: <ul style="list-style-type: none"> <li>• 0—Private Network</li> <li>• 1—Private Network with Guest Access</li> <li>• 2—Chargeable Public Network</li> <li>• 3—Free Public Network</li> <li>• 4—Personal Device Network</li> <li>• 5—Emergency Services Only Network</li> <li>• 14—Test or Experimental</li> <li>• 15—Wildcard</li> </ul>
<i>internet-access</i>	Internet availability status. A value of zero indicates no Internet availability and 1 indicates Internet availability.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the network type and Internet availability on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u network-type 2 1
```

## config wlan hotspot dot11u roam-oi

To configure a roaming consortium Organizational Identifier (OI) list on a 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u roam-oi** command.

```
config wlan hotspot dot11u roam-oi { add wlan_id oi-index oi is-beacon | modify wlan_id oi-index oi is-beacon | delete wlan_id oi-index }
```

### Syntax Description

<b>add</b>	Adds an OI.
<i>wlan-id</i>	Wireless LAN identifier from 1 to 512.
<i>oi-index</i>	Index in the range 1 to 32.
<i>oi</i>	Number that must be a valid 6 digit hexadecimal number and 6 bytes in length. For example, 004096 or AABBDF.
<i>is-beacon</i>	Beacon flag used to add an OI to the beacon. 0 indicates disable and 1 indicates enable. You can add a maximum of 3 OIs for a WLAN with this flag set.
<b>modify</b>	Modifies an OI.
<b>delete</b>	Deletes an OI.

### Command Default

None.

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the roaming consortium OI list:

```
(Cisco Controller) >config wlan hotspot dot11u roam-oi add 4 10 004096 1
```

## config wlan hotspot hs2

To configure the HotSpot2 parameters, use the **config wlan hotspot hs2** command.

```
config wlan hotspot hs2 {disable wlan_id | enable wlan_id | operator-name {add wlan_id index operator_name language-code | delete wlan_id index | modify wlan_id index operator-name language-code} | port-config {add wlan_id port_config_index ip-protocol port-number status | delete wlan_id port-config-index | modify wlan_id port-config-index ip-protocol port-number status} | wan-metrics wlan_id link-status symet-link downlink-speed uplink-speed }
```

Syntax Description		
<b>disable</b>		Disables HotSpot2.
<i>wlan-id</i>		Wireless LAN identifier from 1 to 512.
<b>enable</b>		Enables HotSpot2.
<b>operator-name</b>		Specifies the name of the 802.11 operator.
<b>add</b>		Adds the operator name, port configuration, or WAN metrics parameters to the WLAN configuration.
<i>index</i>		Index of the operator. The range is from 1 to 32.
<i>operator-name</i>		Name of the operator.
<i>language-code</i>		Language used. An ISO-14962-1997 encoded string that defines the language. This string is a three character language code. Enter the first three letters of the language in English. For example, eng for English.
<b>delete</b>		Deletes the operator name, port configuration, or WAN metrics parameters from the WLAN.
<b>modify</b>		Modifies the operator name, port configuration, or WAN metrics parameters of the WLAN.
<b>port-config</b>		Configures the port configuration values.
<i>port_config_index</i>		Port configuration index. The range is from 1 to 32. The default value is 1.
<i>ip-protocol</i>		Protocol to use. This parameter provides information on the connection status of the most commonly used communication protocols and ports. The following options are available: 1—ICMP 6—FTP/SSH/TLS/PPTP-VPN/VoIP 17—IKEv2 (IPSec-VPN/VoIP/ESP) 50—ESP (IPSec-VPN)

<i>port-number</i>	Port number. The following options are available: 0—ICMP/ESP (IPSec-VPN) 20—FTP 22—SSH 443—TLS-VPN 500—IKEv2 1723—PPTP-VPN 4500—IKEv2 5060—VoIP				
<i>status</i>	Status of the IP port. The following options are available: 0—Closed 1—Open 2—Unknown				
<b>wan-metrics</b>	Configures the WAN metrics.				
<i>link-status</i>	Link status. The following options are available: • 0—Unknown • 1—Link up • 2—Link down • 3—Link in test state				
<i>symet-link</i>	Symmetric link status. The following options are available: • 0—Link speed is different for uplink and downlink. For example: ADSL • 1—Link speed is the same for uplink and downlink. For example: DS1				
<i>downlink-speed</i>	Downlink speed of the WAN backhaul link in kbps. Maximum value is 4,194,304 kbps.				
<i>uplink-speed</i>	Uplink speed of the WAN backhaul link in kbps. The maximum value is 4,194,304 kbps.				
<b>Command Default</b>	None				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.6</td> <td>This command was introduced in a release earlier than Release 7.6.</td> </tr> </tbody> </table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				



The following example shows how to configure the WAN metrics parameters:

```
(Cisco Controller) >config wlan hotspot hs2 wan-metrics add 345 1 0 3333
```

## config wlan hotspot msap

To configure the Mobility Service Advertisement Protocol (MSAP) parameters on a WLAN, use the **config wlan hotspot msap** command.

**config wlan hotspot msap** {**enable** | **disable** | **server-id** *server\_id*} *wlan\_id*

### Syntax Description

<b>enable</b>	Enables MSAP on the WLAN.
<b>disable</b>	Disables MSAP on the WLAN.
<b>server-id</b>	Specifies the MSAP server id.
<i>server_id</i>	MSAP server ID. The range is from 1 to 10.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable MSAP on a WLAN:

```
(Cisco Controller) >config wlan hotspot msap enable 4
```

## config wlan interface

To configure a wireless LAN interface or an interface group, use the **config wlan interface** command.

```
config wlan interface {wlan_id | foreignAp} {interface-name | interface-group-name}
```

Syntax Description		
<i>wlan_id</i>	(Optional) Wireless LAN identifier (1 to 512).	
<b>foreignAp</b>	Specifies third-party access points.	
<i>interface-name</i>	Interface name.	
<i>interface-group-name</i>	Interface group name.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an interface named VLAN901:

```
(Cisco Controller) >config wlan interface 16 VLAN901
```

## config wlan ipv6 acl

To configure IPv6 access control list (ACL) on a wireless LAN, use the **config wlan ipv6 acl** command.

**config wlan ipv6 acl** *wlan\_id* *acl\_name*

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<i>acl_name</i>	IPv6 ACL name.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an IPv6 ACL for local switching:

```
(Cisco Controller) >config wlan ipv6 acl 22 acl_sample
```

## config wlan kts-cac

To configure the Key Telephone System-based CAC policy for a WLAN, use the **config wlan kts-cac** command.

```
config wlan kts-cac {enable | disable} wlan_id
```

Syntax Description		
<b>enable</b>	Enables the KTS-based CAC policy.	
<b>disable</b>	Disables the KTS-based CAC policy.	
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

To enable the KTS-based CAC policy for a WLAN, ensure that you do the following:

- Configure the QoS profile for the WLAN to Platinum by entering the following command:  
**config wlan qos wlan-id platinum**
- Disable the WLAN by entering the following command:  
**config wlan disable wlan-id**
- Disable FlexConnect local switching for the WLAN by entering the following command:  
**config wlan flexconnect local-switching wlan-id disable**

The following example shows how to enable the KTS-based CAC policy for a WLAN with the ID 4:

```
(Cisco Controller) >config wlan kts-cac enable 4
```

# config wlan layer2 acl

To configure a Layer 2 access control list (ACL) on a centrally switched WLAN, use the **config wlan acl layer2** command.

```
config wlan layer2 acl wlan_id {acl_name | none}
```

## Syntax Description

<i>wlan_id</i>	Wireless LAN identifier. The range is from 1 to 512.
<i>acl_name</i>	Layer2 ACL name. The name can be up to 32 alphanumeric characters.
<b>none</b>	Clears any Layer2 ACL mapped to the WLAN.

## Command Default

None

## Command History

### Release Modification

7.5	This command was introduced.
-----	------------------------------

## Usage Guidelines

You can create a maximum of 16 rules for a Layer 2 ACL.

You can create a maximum of 64 Layer 2 ACLs on a Cisco WLC.

A maximum of 16 Layer 2 ACLs are supported per access point because an access point supports a maximum of 16 WLANs.

Ensure that the Layer 2 ACL names do not conflict with the FlexConnect ACL names because an access point does not support the same Layer 2 and Layer 3 ACL names.

The following example shows how to apply a Layer 2 ACL on a WLAN:

```
(Cisco Controller) >config wlan layer2 acl 1 acl_12_1
```

## Related Topics

- [config acl counter](#)
- [config acl layer2](#)
- [config ap flexconnect wlan](#)
- [show acl](#)
- [show client detail](#), on page 262
- [show wlan](#), on page 287
- [config wlan layer2 acl](#), on page 134

# config wlan learn-ipaddr-cswlan

To configure client IP address learning on a centrally switched WLAN, use the **config wlan learn-ipaddr-cswlan** command.

```
config wlan learn-ipaddr-cswlan wlan_id {enable | disable}
```

## Syntax Description

*wlan\_id* Wireless LAN identifier from 1 to 512.

**enable** Enables client IPv4 address learning on the centrally switched WLAN

**disable** Disables client IPv4 address learning on the centrally switched WLAN

## Command Default

None

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

## Usage Guidelines

If the client is configured with Layer 2 encryption, the Cisco WLC cannot learn the client IP address and will periodically drop the client. Disable this option so that the Cisco WLC maintains the client connection without waiting to learn the client IP address.

The following example shows how to enable client IP address learning on a centrally switched WLAN:

```
(Cisco Controller) >config wlan learn-ipaddr-cswlan 2 enable
```

## Related Commands

**show wlan**

# config wlan ldap

To add or delete a link to a configured Lightweight Directory Access Protocol (LDAP) server, use the **config wlan ldap** command.

```
config wlan ldap { add wlan_id server_id | delete wlan_id { all | server_id }
```

## Syntax Description

<b>add</b>	Adds a link to a configured LDAP server.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>server_id</i>	LDAP server index.
<b>delete</b>	Removes the link to a configured LDAP server.
<b>all</b>	Specifies all LDAP servers.

## Command Default

None

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

## Usage Guidelines

Use this command to specify the LDAP server priority for the WLAN.

To specify the LDAP server priority, one of the following must be configured and enabled:

- 802.1X authentication and Local EAP
- Web authentication and LDAP



**Note** Local EAP was introduced in controller software release 4.1; LDAP support on Web authentication was introduced in controller software release 4.2.

The following example shows how to add a link to a configured LDAP server with the WLAN ID 100 and server ID 4:

```
(Cisco Controller) >config wlan ldap add 100 4
```



## config wlan load-balance

To override the global load balance configuration and enable or disable load balancing on a particular WLAN, use the **config wlan load-balance** command.

```
config wlan load-balance allow {enable | disable} wlan_id
```

Syntax Description		
<b>enable</b>		Enables band selection on a wireless LAN.
<b>disable</b>		Disables band selection on a wireless LAN.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.

**Command Default** Load balancing is enabled by default.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable band selection on a wireless LAN with WLAN ID 3:

```
(Cisco Controller) >config wlan load-balance allow enable 3
```

## config wlan mac-filtering

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

**config wlan mac-filtering** { **enable** | **disable** } { *wlan\_id* | **foreignAp** }

Syntax Description		
<b>enable</b>	Enables MAC filtering on a wireless LAN.	
<b>disable</b>	Disables MAC filtering on a wireless LAN.	
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.	
<b>foreignAp</b>	Specifies third-party access points.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the MAC filtering on WLAN ID 1:

```
(Cisco Controller) >config wlan mac-filtering enable 1
```

## config wlan max-associated-clients

To configure the maximum number of client connections on a wireless LAN, guest LAN, or remote LAN, use the **config wlan max-associated-clients** command.

```
config wlan max-associated-clients max_clients wlan_id
```

<b>Syntax Description</b>	<i>max_clients</i>	Maximum number of client connections to be accepted.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

<b>Command Default</b>	None
------------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the maximum number of client connections on WLAN ID 2:

```
(Cisco Controller) >config wlan max-associated-clients 25 2
```

## config wlan max-radio-clients

To configure the maximum number of WLAN client per access point, use the **config wlan max-radio-clients** command.

**config wlan max-radio-clients** *max\_radio\_clients wlan\_id*

Syntax Description		
	<i>max_radio_clients</i>	Maximum number of client connections to be accepted per access point radio. The valid range is from 1 to 200.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the maximum number of client connections per access point radio on WLAN ID 2:

```
(Cisco Controller) >config wlan max-radio-clients 25 2
```

## config wlan mdns

To configure an multicast DNS (mDNS) profile for a WLAN, use the **config wlan mdns** command.

```
config wlan mdns {enable | disable | profile {profile-name | none}} {wlan_id | all}
```

### Syntax Description

<b>enable</b>	Enables mDNS snooping on a WLAN.
<b>disable</b>	Disables mDNS snooping on a WLAN.
<b>profile</b>	Configures an mDNS profile for a WLAN.
<i>profile-name</i>	Name of the mDNS profile to be associated with a WLAN.
<b>none</b>	Removes all existing mDNS profiles from the WLAN. You cannot configure mDNS profiles on the WLAN.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
<b>all</b>	Configures the mDNS profile for all WLANs.

### Command Default

By default, mDNS snooping is enabled on WLANs.

### Command History

Release	Modification
7.4	This command was introduced.

### Usage Guidelines

You must disable the WLAN before you use this command. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

The following example shows how to configure an mDNS profile for a WLAN.

```
(Cisco Controller) >config wlan mdns profile profile1 1
```

## config wlan media-stream

To configure multicast-direct for a wireless LAN media stream, use the **config wlan media-stream** command.

**config wlan media-stream multicast-direct** {*wlan\_id* | **all**} {**enable** | **disable**}

Syntax Description		
<b>multicast-direct</b>		Configures multicast-direct for a wireless LAN media stream.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.
<b>all</b>		Configures the wireless LAN on all media streams.
<b>enable</b>		Enables global multicast to unicast conversion.
<b>disable</b>		Disables global multicast to unicast conversion.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** Media stream multicast-direct requires load based Call Admission Control (CAC) to run. WLAN quality of service (QoS) needs to be set to either gold or platinum.

The following example shows how to enable the global multicast-direct media stream with WLAN ID 2:

```
(Cisco Controller) >config wlan media-stream multicast-direct 2 enable
```

## config wlan mfp

To configure management frame protection (MFP) options for the wireless LAN, use the **config wlan mfp** command.

```
config wlan mfp { client [enable | disable] wlan_id | infrastructure protection [enable | disable] wlan_id}
```

Syntax Description		
<b>client</b>		Configures client MFP for the wireless LAN.
<b>enable</b>		(Optional) Enables the feature.
<b>disable</b>		(Optional) Disables the feature.
<i>wlan_id</i>		Wireless LAN identifier (1 to 512).
<b>infrastructure protection</b>		(Optional) Configures the infrastructure MFP for the wireless LAN.

Command Default	
	None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure client management frame protection for WLAN ID 1:

```
(Cisco Controller) >config wlan mfp client enable 1
```

## config wlan mobility foreign-map

To configure interfaces or interface groups for foreign Cisco WLCs, use the **config wlan mobility foreign-map** command.

```
config wlan mobility foreign-map {add | delete} wlan_id foreign_mac_address {interface_name | interface_group_name}
```

Syntax Description		
<b>add</b>		Adds an interface or interface group to the map of foreign controllers.
<b>delete</b>		Deletes an interface or interface group from the map of foreign controllers.
<i>wlan_id</i>		Wireless LAN identifier from 1 to 512.
<i>foreign_mac_address</i>		Foreign switch MAC address on a WLAN.
<i>interface_name</i>		Interface name up to 32 alphanumeric characters.
<i>interface_group_name</i>		Interface group name up to 32 alphanumeric characters.

Command Default	
None	

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add an interface group for foreign Cisco WLCs with WLAN ID 4 and a foreign switch MAC address on WLAN 00:21:1b:ea:36:60:

```
(Cisco Controller) >config wlan mobility foreign-map add 4 00:21:1b:ea:36:60 mygroup1
```



## config wlan multicast buffer

To configure the radio multicast packet buffer size, use the **config wlan multicast buffer** command.

```
config wlan multicast buffer {enable | disable} buffer-size
```

Syntax Description	enable	Description
	<b>enable</b>	Enables the multicast interface feature for a wireless LAN.
	<b>disable</b>	Disables the multicast interface feature on a wireless LAN.
	<i>buffer-size</i>	Radio multicast packet buffer size. The range is from 30 to 60. Enter 0 to indicate APs will dynamically adjust the number of buffers allocated for multicast.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
Command Default	The default buffer size is 30	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure radio multicast buffer settings:

```
(Cisco Controller) >config wlan multicast buffer enable 45 222
```

## config wlan multicast interface

To configure a multicast interface for a wireless LAN, use the **config wlan multicast interface** command.

**config wlan multicast interface** *wlan\_id* { **enable** | **disable** } *interface\_name*

Syntax Description		
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>enable</b>	Enables multicast interface feature for a wireless LAN.
	<b>delete</b>	Disables multicast interface feature on a wireless LAN.
	<i>interface_name</i>	Interface name.
	<b>Note</b>	The interface name can only be specified in lower case characters.

**Command Default** Multicast is disabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the multicast interface feature for a wireless LAN with WLAN ID 4 and interface name myinterface1:

```
(Cisco Controller) >config wlan multicast interface 4 enable myinterface1
```

## config wlan nac

To enable or disable Network Admission Control (NAC) out-of-band support for a WLAN, use the **config wlan nac** command.

```
config wlan nac {snmp | radius} {enable | disable} wlan_id
```

Syntax Description		
<b>snmp</b>		Configures SNMP NAC support.
<b>radius</b>		Configures RADIUS NAC support.
<b>enable</b>		Enables NAC for the WLAN.
<b>disable</b>		Disables NAC for the WLAN.
<i>wlan_id</i>		WLAN identifier from 1 to 512.

Command Default	None
-----------------	------

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** You should enable AAA override before you enable the RADIUS NAC state. You also should disable FlexConnect local switching before you enable the RADIUS NAC state.

The following example shows how to configure SNMP NAC support for WLAN 13:

```
(Cisco Controller) >config wlan nac snmp enable 13
```

The following example shows how to configure RADIUS NAC support for WLAN 34:

```
(Cisco Controller) >config wlan nac radius enable 20
```

## config wlan override-rate-limit

To override the bandwidth limits for upstream and downstream traffic per user and per service set identifier (SSID) defined in the QoS profile, use the **config wlan override-rate-limit** command.

```
config wlan override-rate-limit wlan_id { average-data-rate | average-realtime-rate | burst-data-rate | burst-realtime-rate } { per-ssid | per-client } { downstream | upstream } rate
```

### Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>average-data-rate</b>	Specifies the average data rate for TCP traffic per user or per SSID. The range is from 0 to 51,200 Kbps.
<b>average-realtime-rate</b>	Specifies the average real-time data rate for UDP traffic per user or per SSID. The range is from 0 to 51,200 Kbps.
<b>burst-data-rate</b>	Specifies the peak data rate for TCP traffic per user or per SSID. The range is from 0 to 51,200 Kbps.
<b>burst-realtime-rate</b>	Specifies the peak real-time data rate for UDP traffic per user or per SSID. The range is from 0 to 51,200 Kbps.
<b>per-ssid</b>	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
<b>per-client</b>	Configures the rate limit for each client associated with the SSID.
<b>downstream</b>	Configures the rate limit for downstream traffic.
<b>upstream</b>	Configures the rate limit for upstream traffic.
<i>rate</i>	Data rate for TCP or UDP traffic per user or per SSID. The range is from 0 to 51,200 Kbps. A value of 0 imposes no bandwidth restriction on the QoS profile.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

The rate limits are enforced by the controller and the AP. For central switching, the controller handles the downstream enforcement of per-client rate limit and the AP handles the enforcement of the upstream traffic and per-SSID rate limit for downstream traffic. When the AP enters standalone mode it handles the downstream enforcement of per-client rate limits too.

In FlexConnect local switching and standalone modes, per-client and per-SSID rate limiting is done by the AP for downstream and upstream traffic. However, in FlexConnect standalone mode, the configuration is not saved on the AP, so when the AP reloads, the configuration is lost and rate limiting does not happen after reboot.

For roaming clients, if the client roams between the APs on the same controller, same rate limit parameters are applied on the client. However, if the client roams from an anchor to a foreign controller, the per-client downstream rate limiting uses the parameters configured on the anchor controller while upstream rate limiting uses the parameters of the foreign controller.

The following example shows how to configure the burst real-time actual rate 2000 Kbps for the upstream traffic per SSID:

```
(Cisco Controller) >config wlan override-rate-limit 2 burst-realtime-rate per-ssid upstream  
2000
```

## config wlan passive-client

To configure passive-client feature on a wireless LAN, use the **config wlan passive-client** command.

```
config wlan passive-client { enable | disable } wlan_id
```

Syntax Description		
	<b>enable</b>	Enables the passive-client feature on a WLAN.
	<b>disable</b>	Disables the passive-client feature on a WLAN.
	<i>wlan_id</i>	WLAN identifier between 1 and 512.

Command Default	None
-----------------	------

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** You need to enable the global multicast mode and multicast-multicast mode by using the **config network multicast global** and **config network multicast mode** commands before entering this command.



**Note** You should configure the multicast in multicast-multicast mode only not in unicast mode. The passive client feature does not work with multicast-unicast mode in this release.

The following example shows how to configure the passive client on wireless LAN ID 2:

```
(Cisco Controller) >config wlan passive-client enable 2
```

## config wlan peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **config wlan peer-blocking** command.

```
config wlan peer-blocking { disable | drop | forward-upstream } wlan_id
```

Syntax Description	disable	drop	forward-upstream	wlan_id
	Disables peer-to-peer blocking and bridge traffic locally within the controller whenever possible.	Causes the controller to discard the packets.	Causes the packets to be forwarded on the upstream VLAN. The device above the controller decides what action to take regarding the packets.	WLAN identifier between 1 and 512.
Command Default	None			
Command History	Release	Modification		
	7.6	This command was introduced in a release earlier than Release 7.6.		

The following example shows how to disable the peer-to-peer blocking for WLAN ID 1:

```
(Cisco Controller) >config wlan peer-blocking disable 1
```

## config wlan pmipv6 default-realm

To configure a default realm for a PMIPv6 WLAN, use the **config wlan pmipv6 default-realm** command.

```
config wlan pmipv6 default-realm { default-realm-name | none } wlan_id
```

### Syntax Description

<i>default-realm-name</i>	Default realm name for the WLAN.
<b>none</b>	Clears the realm name for the WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

### Command Default

None.

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default realm name on a PMIPv6 WLAN:

```
(Cisco Controller) >config wlan pmipv6 default-realm XYZ 6
```



## config wlan pmipv6 mobility-type

To configure the mobility type on a WLAN, use the **config wlan pmipv6 mobility-type** command.

```
config wlan pmipv6 mobility-type { none | pmipv6 } { wlan_id | all }
```

### Syntax Description

<b>none</b>	Configures a WLAN with Simple IP mobility.
<b>pmipv6</b>	Configures a WLAN with PMIPv6 mobility.
<b>all</b>	Enables the specified type of mobility for all WLANs.
<i>wlan_id</i>	WLAN identifier between 1 and 512.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

You must disable the WLAN when you configure the mobility type.

The following example shows how to configure the mobility type as PMIPv6 on a WLAN:

```
(Cisco Controller) >config wlan pmipv6 mobility-type pmipv6 16
```

## config wlan pmipv6 profile\_name

To configure a profile name for the PMIPv6 WLAN, use the **config wlan pmipv6 profile\_name** command.

```
config wlan pmipv6 profile_name profile_name wlan_id
```

Syntax Description	
<i>profile_name</i>	Profile name for the PMIPv6 WLAN.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.

Command Default	None
-----------------	------

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** This command binds a profile name to the PMIPv6 WLAN or SSID. Each time that a mobile node associates with the controller, it uses the profile name and NAI in the trigger to the PMIPV6 module. The PMIPV6 module extracts all the profile specific parameters such as LMA IP, APN, and NAI and sends the PBU to the ASR5K.

The following example shows how to create a profile named ABC01 on a PMIPv6 WLAN:

```
(Cisco Controller) >config wlan pmipv6 profile_name ABC01 16
```

# config wlan policy

To configure a policy on a WLAN, use the **config wlan policy** command.

```
config wlan policy {add | delete} priority-index wlan-id
```

Syntax Description		
<b>add</b>		Adds a policy on a WLAN.
<b>delete</b>		Deletes an existing policy from a WLAN.
<i>priority-index</i>		Priority index of the policy to be configured on the WLAN. The policies are applied to the clients according to the priority index. The range is from 1 to 16.
<i>policy_name</i>		Name of the profiling policy.
<i>wlan-id</i>		WLAN identifier from 1 to 512.

**Command Default** There is no WLAN policy.

Command History	Release	Modification
	7.5	This command was introduced.

**Usage Guidelines** You can apply up to 16 policies on a WLAN.

The following example shows how to configure a policy on a WLAN:

```
(Cisco Controller) >config wlan policy add 1 teacher_policy 1
```

## Related Topics

- [config policy](#)
- [debug policy](#)
- [show policy](#)

# config wlan profiling

To configure client profiling on a WLAN, use the **config wlan profiling** command.

**config wlan profiling** {local | radius} {all | dhcp | http} {enable | disable} *wlan\_id*

## Syntax Description

<b>local</b>	Configures client profiling in Local mode for a WLAN.
<b>radius</b>	Configures client profiling in RADIUS mode on a WLAN.
<b>all</b>	Configures DHCP and HTTP client profiling in a WLAN.
<b>dhcp</b>	Configures DHCP client profiling alone in a WLAN.
<b>http</b>	Configures HTTP client profiling in a WLAN.
<b>enable</b>	Enables the specific type of client profiling in a WLAN.  When you enable HTTP profiling, the Cisco WLC collects the HTTP attributes of clients for profiling.  When you enable DHCP profiling, the Cisco WLC collects the DHCP attributes of clients for profiling.
<b>disable</b>	Disables the specific type of client profiling in a WLAN.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.

## Usage Guidelines

Ensure that you have disabled the WLAN before configuring client profiling on the WLAN.

## Command Default

Client profiling is disabled.

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

## Usage Guidelines

Only clients connected to port 80 for HTTP can be profiled. IPv6 only clients are not profiled.

If a session timeout is configured for a WLAN, clients must send the HTTP traffic before the configured timeout to get profiled.

This feature is not supported on the following:

- FlexConnect Standalone mode
- FlexConnect Local Authentication

The following example shows how to enable both DHCP and HTTP profiling on a WLAN:

```
(Cisco Controller) >config wlan profiling radius all enable 6
HTTP Profiling successfully enabled.
DHCP Profiling successfully enabled.
```

## config wlan qos

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

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

Syntax Description		
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>bronze</b>	Specifies the bronze QoS policy.
	<b>silver</b>	Specifies the silver QoS policy.
	<b>gold</b>	Specifies the gold QoS policy.
	<b>platinum</b>	Specifies the platinum QoS policy.
	<b>foreignAp</b>	Specifies third-party access points.

**Command Default** The default QoS policy is silver.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the highest level of service on wireless LAN 1:

```
(Cisco Controller) >config wlan qos 1 gold
```

## config wlan radio

To set the Cisco radio policy on a wireless LAN, use the **config wlan radio** command.

**config wlan radio** *wlan\_id* { **all** | **802.11a** | **802.11bg** | **802.11g** | **802.11ag** }

### Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>all</b>	Configures the wireless LAN on all radio bands.
<b>802.11a</b>	Configures the wireless LAN on only 802.11a.
<b>802.11bg</b>	Configures the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled).
<b>802.11g</b>	Configures the wireless LAN on 802.11g only.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the wireless LAN on all radio bands:

```
(Cisco Controller) >config wlan radio 1 all
```

## config wlan radius\_server acct

To configure RADIUS accounting servers of a WLAN, use the **config wlan radius\_server acct** command.

```
config wlan radius_server acct {enable | disable} wlan_id | add wlan_id server_id | delete wlan_id
{all | server_id} | framed-ipv6 { address | both | prefix } wlan_id}
```

Syntax Description		
<b>enable</b>	Enables RADIUS accounting for the WLAN.	
<b>disable</b>	Disables RADIUS accounting for the WLAN.	
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.	
<b>add</b>	Adds a link to a configured RADIUS accounting server.	
<i>server_id</i>	RADIUS server index.	
<b>delete</b>	Deletes a link to a configured RADIUS accounting server.	
<b>address</b>	Configures an accounting framed IPv6 attribute to an IPv6 address.	
<b>both</b>	Configures the accounting framed IPv6 attribute to an IPv6 address and prefix.	
<b>prefix</b>	Configures the accounting framed IPv6 attribute to an IPv6 prefix.	
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable RADIUS accounting for the WLAN 2:

```
(Cisco Controller) >config wlan radius_server acct enable 2
```

The following example shows how to add a link to a configured RADIUS accounting server:

```
(Cisco Controller) > config wlan radius_server acct add 2 5
```

## config wlan radius\_server acct interim-update

To configure the interim update of a RADIUS accounting server of a WLAN, use the **config wlan radius\_server acct interim-update** command.

```
config wlan radius_server acct interim-update {enable | disable | interval} wlan_id
```

Syntax Description		
<b>interim-update</b>		Configures the interim update of the RADIUS accounting server.
<b>enable</b>		Enables interim update of the RADIUS accounting server for the WLAN.
<b>disable</b>		Disables interim update of the RADIUS accounting server for the WLAN.
<i>interval</i>		Interim update interval that you specify. The valid range is 180 seconds to 3600 seconds.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.

**Command Default** Interim update of a RADIUS accounting sever is set at 600 seconds.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify an interim update of 200 seconds to a RADIUS accounting server of WLAN 2:

```
(Cisco Controller) >config wlan radius_server acct interim-update 200 2
```



## config wlan radius\_server auth

To configure RADIUS authentication servers of a WLAN, use the **config wlan radius\_server auth** command.

```
config wlan radius_server auth {enable wlan_id | disable wlan_id} {add wlan_id server_id | delete wlan_id {all | server_id}}
```

Syntax	Description
<b>auth</b>	Configures a RADIUS authentication
<b>enable</b>	Enables RADIUS authentication for this WLAN.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
<b>disable</b>	Disables RADIUS authentication for this WLAN.
<b>add</b>	Adds a link to a configured RADIUS server.
<i>server_id</i>	RADIUS server index.
<b>delete</b>	Deletes a link to a configured RADIUS server.
<b>all</b>	Deletes all links to configured RADIUS servers.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a link to a configured RADIUS authentication server with WLAN ID 1 and Server ID 1:

```
(Cisco Controller) >config wlan radius_server auth add 1 1
```

## config wlan radius\_server acct interim-update

To configure the interim update of a RADIUS accounting server of a WLAN, use the **config wlan radius\_server acct interim-update** command.

**config wlan radius\_server acct interim-update** { **enable** | **disable** | *interval* } *wlan\_id*

Syntax Description		
<b>interim-update</b>		Configures the interim update of the RADIUS accounting server.
<b>enable</b>		Enables interim update of the RADIUS accounting server for the WLAN.
<b>disable</b>		Disables interim update of the RADIUS accounting server for the WLAN.
<i>interval</i>		Interim update interval that you specify. The valid range is 180 seconds to 3600 seconds.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.

**Command Default** Interim update of a RADIUS accounting sever is set at 600 seconds.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify an interim update of 200 seconds to a RADIUS accounting server of WLAN 2:

```
(Cisco Controller) >config wlan radius_server acct interim-update 200 2
```

## config wlan radius\_server overwrite-interface

To configure a wireless LAN's RADIUS dynamic interface, use the **config wlan radius\_server overwrite-interface** command.

```
config wlan radius_server overwrite-interface {apgroup | enable | disable | wlan} wlan_id
```

Syntax Description		
<b>apgroup</b>		Enables AP group's interface for all RADIUS traffic on the WLAN.
<b>enable</b>		Enables RADIUS dynamic interface for this WLAN.
<b>disable</b>		Disables RADIUS dynamic interface for this WLAN.
<b>wlan</b>		Enables WLAN's interface for all RADIUS traffic on the WLAN.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** The controller uses the management interface as identity. If the RADIUS server is on a directly connected dynamic interface, the traffic is sourced from the dynamic interface. Otherwise, the management IP address is used.

If the feature is enabled, controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on the WLAN.

The following example shows how to enable RADIUS dynamic interface for a WLAN with an ID 1:

```
(Cisco Controller) >config wlan radius_server overwrite-interface enable 1
```

## config wlan roamed-voice-client re-anchor

To configure a roamed voice client's reanchor policy, use the **config wlan roamed-voice-client re-anchor** command.

**config wlan roamed-voice-client re-anchor** {enable | disable} *wlan\_id*

Syntax Description		
<b>enable</b>		Enables the roamed client's reanchor policy.
<b>disable</b>		Disables the roamed client's reanchor policy.
<i>wlan_id</i>		Wireless LAN identifier between 1 and 512.

**Command Default** The roamed client reanchor policy is disabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a roamed voice client's reanchor policy where WLAN ID is 1:

```
(Cisco Controller) >config wlan roamed-voice-client re-anchor enable 1
```

## config wlan security 802.1X

To change the state of 802.1X security on the wireless LAN Cisco radios, use the **config wlan security 802.1X** command.

```
config wlan security 802.1X {enable {wlan_id | foreignAp} | disable {wlan_id | foreignAp}
| encryption {wlan_id | foreignAp} {0 | 40 | 104} | on-macfilter-failure {enable | disable}}
```

Syntax	Description
<b>enable</b>	Enables the 802.1X settings.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>foreignAp</b>	Specifies third-party access points.
<b>disable</b>	Disables the 802.1X settings.
<b>encryption</b>	Specifies the static WEP keys and indexes.
<b>0</b>	Specifies a WEP key size of 0 (no encryption) bits. The default value is 104.  <b>Note</b> All keys within a wireless LAN must be the same size.
<b>40</b>	Specifies a WEP key size of 40 bits. The default value is 104.  <b>Note</b> All keys within a wireless LAN must be the same size.
<b>104</b>	Specifies a WEP key size of 104 bits. The default value is 104.  <b>Note</b> All keys within a wireless LAN must be the same size.
<b>on-macfilter-failure</b>	Configures 802.1X on MAC filter failure.
<b>enable</b>	Enables 802.1X authentication on MAC filter failure.
<b>disable</b>	Disables 802.1X authentication on MAC filter failure.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** To change the encryption level of 802.1X security on the wireless LAN Cisco radios, use the following key sizes:

- 0—no 802.1X encryption.
- 40—40/64-bit encryption.
- 104—104/128-bit encryption. (This is the default encryption setting.)

The following example shows how to configure 802.1X security on WLAN ID 16.

```
(Cisco Controller) >config wlan security 802.1X enable 16
```

## config wlan security ckip

To configure Cisco Key Integrity Protocol (CKIP) security options for the wireless LAN, use the **config wlan security ckip** command.

```
config wlan security ckip {enable | disable} wlan_id [akm psk set-key {hex | ascii} {40 | 104} key key_index wlan_id | mmh-mic {enable | disable} wlan_id | kp {enable | disable} wlan_id]
```

Syntax Description		
<b>enable</b>		Enables CKIP security.
<b>disable</b>		Disables CKIP security.
<i>wlan_id</i>		Wireless LAN identifier from 1 to 512.
<b>akm psk set-key</b>		(Optional) Configures encryption key management for the CKIP wireless LAN.
<b>hex</b>		Specifies a hexadecimal encryption key.
<b>ascii</b>		Specifies an ASCII encryption key.
<b>40</b>		Sets the static encryption key length to 40 bits for the CKIP WLAN. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters.
<b>104</b>		Sets the static encryption key length to 104 bits for the CKIP WLAN. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.
<b>key</b>		Specifies the CKIP WLAN key settings.
<i>key_index</i>		Configured PSK key index.
<b>mmh-mic</b>		(Optional) Configures multi-modular hash message integrity check (MMH MIC) validation for the CKIP wireless LAN.
<b>kp</b>		(Optional) Configures key-permutation for the CKIP wireless LAN.

**Command Default** None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a CKIP WLAN encryption key of 104 bits (26 hexadecimal characters) for PSK key index 2 on WLAN 03:

```
(Cisco Controller) >config wlan security ckip akm psk set-key hex 104 key 2 03
```

## config wlan security cond-web-redir

To enable or disable conditional web redirect, use the **config wlan security cond-web-redir** command.

**config wlan security cond-web-redir** { **enable** | **disable** } *wlan\_id*

Syntax Description		
<b>enable</b>	Enables conditional web redirect.	
<b>disable</b>	Disables conditional web redirect.	
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the conditional web direct on WLAN ID 2:

```
(Cisco Controller) >config wlan security cond-web-redir enable 2
```



## config wlan security eap-passthru

To configure the 802.1X frames pass through on to the external authenticator, use the **config wlan security eap-passthru** command.

```
config wlan security eap-passthru {enable | disable} wlan_id
```

Syntax Description	enable	disable	wlan_id
	Enables 802.1X frames pass through to external authenticator.	Disables 802.1X frames pass through to external authenticator.	Wireless LAN identifier between 1 and 512.
Command Default	None		
Command History	Release	Modification	
	7.6	This command was introduced in a release earlier than Release 7.6.	

The following example shows how to enable the 802.1X frames pass through to external authenticator on WLAN ID 2:

```
(Cisco Controller) >config wlan security eap-passthru enable 2
```

## config wlan security ft

To configure 802.11r Fast Transition Roaming parameters, use the **config wlan security ft** command.

**config wlan security ft** { **enable** | **disable** | **reassociation-timeout** *timeout-in-seconds* } *wlan\_id*

### Syntax Description

<b>enable</b>	Enables 802.11r Fast Transition Roaming support.
<b>disable</b>	Disables 802.11r Fast Transition Roaming support.
<b>reassociation-timeout</b>	Configures reassociation deadline interval.
<i>timeout-in-seconds</i>	Reassociation timeout value, in seconds. The valid range is 1 to 100 seconds.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

The following example shows how to enable 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft enable 2
```

The following example shows how to set a reassociation timeout value of 20 seconds for 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft reassociation-timeout 20 2
```

## config wlan security ft over-the-ds

To configure 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** command.

```
config wlan security ft over-the-ds {enable | disable} wlan_id
```

Syntax Description	enable	enable
	enable	Enables 802.11r fast transition roaming support over a distributed system.
	disable	Disables 802.11r fast transition roaming support over a distributed system.
	wlan_id	Wireless LAN identifier between 1 and 512.

**Command Default** Enabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** Ensure that you have disabled the WLAN before you proceed.  
Ensure that 802.11r fast transition is enabled on the WLAN.

The following example shows how to enable 802.11r fast transition roaming support over a distributed system on WLAN ID 2:

```
(Cisco Controller) >config wlan security ft over-the-ds enable 2
```

## config wlan security IPsec disable

To disable IPsec security, use the **config wlan security IPsec disable** command.

**config wlan security IPsec disable** { *wlan\_id* | **foreignAp** }

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>foreignAp</b>	Specifies third-party access points.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the IPsec for WLAN ID 16:

```
(Cisco Controller) >config wlan security IPsec disable 16
```

## config wlan security IPsec enable

To enable IPsec security, use the **config wlan security IPsec enable** command.

```
config wlan security IPsec enable {wlan_id | foreignAp}
```

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>foreignAp</b>	Specifies third-party access points.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the IPsec for WLAN ID 16:

```
(Cisco Controller) >config wlan security IPsec enable 16
```

## config wlan security IPsec authentication

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

```
config wlan security IPsec authentication { hmac-md5 | hmac-sha-1 } { wlan_id | foreignAp }
```

Syntax Description		
<b>hmac-md5</b>	Specifies the IPsec HMAC-MD5 authentication protocol.	
<b>hmac-sha-1</b>	Specifies the IPsec HMAC-SHA-1 authentication protocol.	
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
<b>foreignAp</b>	Specifies third-party access points.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec HMAC-SHA-1 security authentication parameter for WLAN ID 1:

```
(Cisco Controller) >config wlan security IPsec authentication hmac-sha-1 1
```

## config wlan security IPsec encryption

To modify the IPsec security encryption protocol used on the wireless LAN, use the **config wlan security IPsec encryption** command.

```
config wlan security IPsec encryption {3des | aes | des} {wlan_id | foreignAp}
```

Syntax Description	3des	Enables IPsec 3DES encryption.
	<b>aes</b>	Enables IPsec AES 128-bit encryption.
	<b>des</b>	Enables IPsec DES encryption.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>foreignAp</b>	Specifies third-party access points.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec AES encryption:

```
(Cisco Controller) >config wlan security IPsec encryption aes 1
```

## config wlan security IPsec config

To configure the proprietary Internet Key Exchange (IKE) CFG-Mode parameters used on the wireless LAN, use the **config wlan security IPsec config** command.

```
config wlan security IPsec config qotd ip_address {wlan_id | foreignAp}
```

Syntax Description		
<b>qotd</b>	Configures the quote-of-the-day server IP for cfg-mode.	
<i>ip_address</i>	Quote-of-the-day server IP for cfg-mode.	
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
<b>foreignAp</b>	Specifies third-party access points.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

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

The following example shows how to configure the quote-of-the-day server IP 44.55.66.77 for cfg-mode for WLAN 1:

```
(Cisco Controller) >config wlan security IPsec config qotd 44.55.66.77 1
```



## config wlan security IPsec ike authentication

To modify the IPsec Internet Key Exchange (IKE) authentication protocol used on the wireless LAN, use the **config wlan security IPsec ike authentication** command.

```
config wlan security IPsec ike authentication {certificates {wlan_id | foreignAp} | pre-share-key
{wlan_id | foreignAp} key | xauth-psk {wlan_id | foreignAp} key}
```

Syntax Description	Parameter	Description
	<b>certificates</b>	Enables the IKE certificate mode.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>foreignAp</b>	Specifies third-party access points.
	<b>pre-share-key</b>	Enables the IKE Xauth with preshared keys.
	<b>xauth-psk</b>	Enables the IKE preshared key.
	<i>key</i>	Key required for preshare and xauth-psk.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IKE certification mode:

```
(Cisco Controller) >config wlan security IPsec ike authentication certificates 16
```

## config wlan security IPsec ike dh-group

To modify the IPsec Internet Key Exchange (IKE) Diffie Hellman group used on the wireless LAN, use the **config wlan security IPsec ike dh-group** command.

**config wlan security IPsec ike dh-group** {*wlan\_id* | **foreignAp**} {**group-1** | **group-2** | **group-5**}

### Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>foreignAp</b>	Specifies third-party access points.
<b>group-1</b>	Specifies DH group 1 (768 bits).
<b>group-2</b>	Specifies DH group 2 (1024 bits).
<b>group-5</b>	Specifies DH group 5 (1536 bits).

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the Diffie Hellman group parameter for group-1:

```
(Cisco Controller) >config wlan security IPsec ike dh-group 1 group-1
```

## config wlan security IPsec ike lifetime

To modify the IPsec Internet Key Exchange (IKE) lifetime used on the wireless LAN, use the **config wlan security IPsec ike lifetime** command.

```
config wlan security IPsec ike lifetime {wlan_id | foreignAp} seconds
```

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>foreignAp</b>	Specifies third-party access points.
	<i>seconds</i>	IKE lifetime in seconds, between 1800 and 345600.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec IKE lifetime use on the wireless LAN:

```
(Cisco Controller) >config wlan security IPsec ike lifetime 1 1900
```

## config wlan security IPsec ike phase1

To modify IPsec Internet Key Exchange (IKE) Phase 1 used on the wireless LAN, use the **config wlan security IPsec ike phase1** command.

```
config wlan security IPsec ike phase1 {aggressive | main} {wlan_id | foreignAp}
```

Syntax Description		
<b>aggressive</b>	Enables the IKE aggressive mode.	
<b>main</b>	Enables the IKE main mode.	
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
<b>foreignAp</b>	Specifies third-party access points.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to modify IPsec IKE Phase 1:

```
(Cisco Controller) >config wlan security IPsec ike phase1 aggressive 16
```

## config wlan security IPsec ike contivity

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

```
config wlan security IPsec ike contivity {enable | disable} {wlan_id | foreignAp}
```

Syntax Description		
<b>enable</b>	Enables contivity support for this WLAN.	
<b>disable</b>	Disables contivity support for this WLAN.	
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
<b>foreignAp</b>	Specifies third-party access points.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to modify Contivity VPN client support:

```
(Cisco Controller) >config wlan security IPsec ike contivity enable 14
```

## config wlan security passthru

To modify the IPsec pass-through used on the wireless LAN, use the **config wlan security passthru** command.

```
config wlan security passthru { enable | disable } { wlan_id | foreignAp } [ip_address]
```

### Syntax Description

<b>enable</b>	Enables IPsec pass-through.
<b>disable</b>	Disables IPsec pass-through.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>foreignAp</b>	Specifies third-party access points.
<i>ip_address</i>	(Optional) IP address of the IPsec gateway (router) that is terminating the VPN tunnel.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to modify IPsec pass-through used on the wireless LAN:

```
(Cisco Controller) >config wlan security passthru enable 3 192.12.1.1
```

## config wlan security pmf

To configure 802.11w Management Frame Protection (MFP) on a WLAN, use the **config wlan security pmf** command.

```
config wlan security pmf {disable | optional | required | association-comeback
association-comeback_timeout | saquery-retrytimeout saquery-retry_timeout} wlan_id
```

Syntax Description		
<b>disable</b>		Disables 802.11w MFP protection on a WLAN.
<b>optional</b>		Enables 802.11w MFP protection on a WLAN.
<b>required</b>		Requires clients to negotiate 802.11w MFP protection on a WLAN.
<b>association-comeback</b>		Configures the 802.11w association comeback time.
<i>association-comeback_timeout</i>		Association comeback interval in seconds. Time interval that an associated client must wait before the association is tried again after it is denied with a status code 30. The status code 30 message is "Association request rejected temporarily; Try again later".  The range is from 1 to 20 seconds.
<b>saquery-retrytimeout</b>		Configures the 802.11w Security Association (SA) query retry timeout.
<i>saquery-retry_timeout</i>		Time interval identified in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the controller. The range is from 100 to 500 ms.
<i>wlan_id</i>		Wireless LAN identifier from 1 to 512.

**Command Default**

Default SA query retry timeout is 200 milliseconds.  
Default association comeback timeout is 1 second.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines**

802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast robust management frames. IGTK is a random value, assigned by the authenticator station (controller) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is derived using the four way handshake and is used only on WLANs that are configured with WPA or WPA2 security at Layer 2.

The following example shows how to enable 802.11w MFP protection on a WLAN:

```
(Cisco Controller) > config wlan security pmf optional 1
```

The following example shows how to configure the SA query retry timeout on a WLAN:

```
(Cisco Controller) > config wlan security pmf saquery-retrytimeout 300 1
```



## config wlan security splash-page-web-redirect

To enable or disable splash page web redirect, use the **config wlan security splash-page-web-redirect** command.

```
config wlan security splash-page-web-redirect {enable | disable} wlan_id
```

Syntax	Description
<b>enable</b>	Enables splash page web redirect.
<b>disable</b>	Disables splash page web redirect.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

**Command Default** Splash page web redirect is disabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable splash page web redirect:

```
(Cisco Controller) >config wlan security splash-page-web-redirect enable 2
```

## config wlan security static-wep-key authentication

To configure static Wired Equivalent Privacy (WEP) key 802.11 authentication on a wireless LAN, use the **config wlan security static-wep-key authentication** command.

**config wlan security static-wep-key authentication** { **shared-key** | **open** } *wlan\_id*

Syntax Description		
<b>shared-key</b>	Enables shared key authentication.	
<b>open</b>	Enables open system authentication.	
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the static WEP shared key authentication for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key authentication shared-key 1
```

## config wlan security static-wep-key disable

To disable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key disable** command.

```
config wlan security static-wep-key disable wlan_id
```

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the static WEP keys for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key disable 1
```

## config wlan security static-wep-key enable

To enable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key enable** command.

**config wlan security static-wep-key enable** *wlan\_id*

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the use of static WEK keys for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key enable 1
```

## config wlan security static-wep-key encryption

To configure the static Wired Equivalent Privacy (WEP) keys and indexes, use the **config wlan security static-wep-key encryption** command.

```
config wlan security static-wep-key encryption wlan_id {40 | 104} {hex | ascii} key key-index
```

Syntax Description		
<i>wlan_id</i>		Wireless LAN identifier from 1 to 512.
<b>40</b>		Specifies the encryption level of 40.
<b>104</b>		Specifies the encryption level of 104.
<b>hex</b>		Specifies to use hexadecimal characters to enter key.
<b>ascii</b>		Specifies whether to use ASCII characters to enter key.
<i>key</i>		WEP key in ASCII.
<i>key-index</i>		Key index (1 to 4).

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** One unique WEP key index can be applied to each wireless LAN. Because there are only four WEP key indexes, only four wireless LANs can be configured for static WEP Layer 2 encryption.

Make sure to disable 802.1X before using this command.

The following example shows how to configure the static WEP keys for WLAN ID 1 that uses hexadecimal character 0201702001 and key index 2:

```
(Cisco Controller) >config wlan security static-wep-key encryption 1 40 hex 0201702001 2
```

## config wlan security tkip

To configure the Temporal Key Integrity Protocol (TKIP) Message Integrity Check (MIC) countermeasure hold-down timer, use the **config wlan security tkip** command.

**config wlan security tkip hold-down** *time wlan\_id*

Syntax Description	hold-down	Configures the TKIP MIC countermeasure hold-down timer.
	<i>time</i>	TKIP MIC countermeasure hold-down time in seconds. The range is from 0 to 60 seconds.
	<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.

**Command Default** The default TKIP countermeasure is set to 60 seconds.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** TKIP countermeasure mode can occur if the access point receives 2 MIC errors within a 60 second period. When this situation occurs, the access point deauthenticates all TKIP clients that are associated to that 802.11 radio and holds off any clients for the countermeasure holdoff time.

The following example shows how to configure the TKIP MIC countermeasure hold-down timer:

```
(Cisco Controller) >config wlan security tkip
```

## config wlan security web-auth

To change the status of web authentication used on a wireless LAN, use the **config wlan security web-auth** command.

```
config wlan security web-auth {{acl | enable | disable} {wlan_id | foreignAp} [acl_name | none]} | {on-macfilter-failure wlan_id} | {server-precedence wlan_id | local | ldap | radius} | {flexacl wlan_id [ipv4_acl_name | none]} | {ipv6 acl wlan_id [ipv6_acl_name | none]} | {mac-auth-server {ip_address wlan_id}} | {timeout {value_in_seconds wlan_id}} | {web-portal-server {ip_address wlan_id}}
```

Syntax	Description
<b>acl</b>	Configures the access control list.
<b>enable</b>	Enables web authentication.
<b>disable</b>	Disables web authentication.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
<b>foreignAp</b>	Specifies third-party access points.
<i>acl_name</i>	(Optional) ACL name (up to 32 alphanumeric characters).
<b>none</b>	(Optional) Specifies no ACL name.
<b>on-macfilter-failure</b>	Enables web authentication on MAC filter failure.
<b>server-precedence</b>	Configures the authentication server precedence order for Web-Auth users.
<b>local</b>	Specifies the server type.
<b>ldap</b>	Specifies the server type.
<b>radius</b>	Specifies the server type.
<b>flexacl</b>	Configures Flexconnect Access Control List.
<i>ipv4_acl_name</i>	(Optional) IPv4 ACL name. You can enter up to 32 alphanumeric characters.
<i>ipv6_acl_name</i>	(Optional) IPv6 ACL name. You can enter up to 32 alphanumeric characters.
<i>ipv6</i>	Configures IPv6 related parameters.
<b>mac-auth-server</b>	Configures MAC authentication server for the WLAN.
<b>timeout</b>	Configures Local Web authentication Timeout. <b>Note</b> The CWA session timeout is fixed to 600 seconds.

---

<i>value_in_seconds</i>	Timeout value in seconds; valid range is between 300 and 14400 seconds.
-------------------------	---

---

<b>web-portal-server</b>	Configures CMCC web portal server for the WLAN.
--------------------------	---

---

**Command Default**

None

**Command History**

<b>Release</b>	<b>Modification</b>
7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to configure the security policy for WLAN ID 1 and an ACL named ACL03:

```
(Cisco Controller) >config wlan security web-auth acl 1 ACL03
```



## config wlan security web-passthrough acl

To add an access control list (ACL) to the wireless LAN definition, use the **config wlan security web-passthrough acl** command.

```
config wlan security web-passthrough acl {wlan_id | foreignAp} {acl_name | none}
```

Syntax Description		
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
<b>foreignAp</b>	Specifies third-party access points.	
<i>acl_name</i>	ACL name (up to 32 alphanumeric characters).	
<b>none</b>	Specifies that there is no ACL.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add an ACL to the wireless LAN definition:

```
(Cisco Controller) >config wlan security web-passthrough acl 1 ACL03
```

## config wlan security web-passthrough disable

To disable a web captive portal with no authentication required on a wireless LAN, use the **config wlan security web-passthrough disable** command.

**config wlan security web-passthrough disable** {*wlan\_id* | **foreignAp**}

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>foreignAp</b>	Specifies third-party access points.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable a web captive portal with no authentication required on wireless LAN ID 1:

```
(Cisco Controller) >config wlan security web-passthrough disable 1
```

## config wlan security web-passthrough email-input

To configure a web captive portal using an e-mail address, use the **config wlan security web-passthrough email-input** command.

```
config wlan security web-passthrough email-input {enable | disable} {wlan_id | foreignAp}
```

Syntax Description	email-input	Configures a web captive portal using an e-mail address.
	<b>enable</b>	Enables a web captive portal using an e-mail address.
	<b>disable</b>	Disables a web captive portal using an e-mail address.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>foreignAp</b>	Specifies third-party access points.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a web captive portal using an e-mail address:

```
(Cisco Controller) >config wlan security web-passthrough email-input enable 1
```

## config wlan security web-passthrough enable

To enable a web captive portal with no authentication required on the wireless LAN, use the **config wlan security web-passthrough enable** command.

**config wlan security web-passthrough enable** {*wlan\_id* | **foreignAp**}

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
	<b>foreignAp</b>	Specifies third-party access points.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a web captive portal with no authentication required on wireless LAN ID 1:

```
(Cisco Controller) >config wlan security web-passthrough enable 1
```

## config wlan security wpa akm 802.1x

To configure authentication key-management (AKM) using 802.1X, use the **config wlan security wpa akm 802.1x** command.

```
config wlan security wpa akm 802.1x {enable | disable} wlan_id
```

Syntax Description	enable	Disables the 802.1X support.
	disable	Disables the 802.1X support.
	wlan_id	Wireless LAN identifier from 1 to 512.

  

Command Default	None
-----------------	------

  

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure authentication using 802.1X.

```
(Cisco Controller) >config wlan security wpa akm 802.1x enable 1
```

## config wlan security wpa akm cckm

To configure authentication key-management using Cisco Centralized Key Management (CCKM), use the `config wlan security wpa akm cckm` command.

```
config wlan security wpa akm cckm { enable wlan_id | disable wlan_id | timestamp-tolerance }
```

Syntax Description		
<b>enable</b>	Enables CCKM support.	
<b>disable</b>	Disables CCKM support.	
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
<i>timestamp-tolerance</i>	CCKM IE time-stamp tolerance. The range is between 1000 to 5000 milliseconds; the default is 1000 milliseconds.	
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure authentication key-management using CCKM.

```
(Cisco Controller) >config wlan security wpa akm cckm 1500
```

## config wlan security wpa akm ft

To configure authentication key-management using 802.11r fast transition 802.1X, use the **config wlan security wpa akm ft** command.

```
config wlan security wpa akm ft [over-the-air | over-the-ds | psk | [reassociation-timeout seconds]]
{enable | disable} wlan_id
```

Syntax	Description
<b>over-the-air</b>	(Optional) Configures 802.11r fast transition roaming over-the-air support.
<b>over-the-ds</b>	(Optional) Configures 802.11r fast transition roaming DS support.
<b>psk</b>	(Optional) Configures 802.11r fast transition PSK support.
<b>reassociation-timeout</b>	(Optional) Configures the reassociation deadline interval.  The valid range is between 1 to 100 seconds. The default value is 20 seconds.
<i>seconds</i>	Reassociation deadline interval in seconds.
<b>enable</b>	Enables 802.11r fast transition 802.1X support.
<b>disable</b>	Disables 802.11r fast transition 802.1X support.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure authentication key-management using 802.11r fast transition:

```
(Cisco Controller) >config wlan security wpa akm ft reassociation-timeout 25 1
```

## config wlan security wpa akm pmf

To configure Authenticated Key Management (AKM) of management frames, use the **config wlan security wpa akm pmf** command.

```
config wlan security wpa akm pmf {802.1x | psk} {enable | disable} wlan_id
```

### Syntax Description

**802.1x** Configures 802.1X authentication for protection of management frames (PMF).

**psk** Configures preshared keys (PSK) for PMF.

**enable** Enables 802.1X authentication or PSK for PMF.

**disable** Disables 802.1X authentication or PSK for PMF.

*wlan\_id* Wireless LAN identifier from 1 to 512.

### Command Default

Disabled.

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

802.11w has two new AKM suites: 00-0F-AC:5 or 00-0F-AC:6. You must enable WPA and then disable the WLAN to configure PMF on the WLAN.

The following example shows how to enable 802.1X authentication for PMF in a WLAN:

```
(Cisco Controller) >config wlan security wpa akm pmf 802.1x enable 1
```



## config wlan security wpa akm psk

To configure the Wi-Fi protected access (WPA) preshared key mode, use the **config wlan security wpa akm psk** command.

```
config wlan security wpa akm psk { enable | disable | set-key key-format key } wlan_id
```

Syntax Description		
<b>enable</b>	Enables WPA-PSK.	
<b>disable</b>	Disables WPA-PSK.	
<b>set-key</b>	Configures a preshared key.	
<i>key-format</i>	Specifies key format. Either ASCII or hexadecimal.	
<i>key</i>	WPA preshared key.	
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the WPA preshared key mode:

```
(Cisco Controller) >config wlan security wpa akm psk disable 1
```

## config wlan security wpa disable

To disable WPA1, use the **config wlan security wpa disable** command.

**config wlan security wpa disable** *wlan\_id*

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable WPA:

```
(Cisco Controller) >config wlan security wpa disable 1
```

## config wlan security wpa enable

To enable WPA1, use the **config wlan security wpa enable** command.

**config wlan security wpa enable** *wlan\_id*

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the WPA on WLAN ID 1:

```
(Cisco Controller) >config wlan security wpa enable 1
```

## config wlan security wpa ciphers

To configure the Wi-Fi protected authentication (WPA1) or Wi-Fi protected authentication (WPA2), use the `config wlan security wpa ciphers` command.

```
config wlan security wpa { wpa1 | wpa2 } ciphers { aes | tkip } { enable | disable } wlan_id
```

Syntax Description		
	<b>wpa1</b>	Configures WPA1 support.
	<b>wpa2</b>	Configures WPA2 support.
	<b>ciphers</b>	Configures WPA ciphers.
	<b>aes</b>	Configures AES encryption support.
	<b>tkip</b>	Configures TKIP encryption support.
	<b>enable</b>	Enables WPA AES/TKIP mode.
	<b>disable</b>	Disables WPA AES/TKIP mode.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default	None
-----------------	------

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

- Usage Guidelines**
- If you are not specifying the WPA versions, it implies the following:
- If the cipher enabled is AES, you are configuring WPA2/AES.
  - If the ciphers enabled is AES+TKIP, you are configuring WPA/TKIP, WPA2/AES, or WPA/TKIP.
  - If the cipher enabled is TKIP, you are configuring WPA/TKIP or WPA2/TKIP.

The following example shows how to encrypt the WPA:

```
(Cisco Controller) >config wlan security wpa wpa1 ciphers aes enable 1
```

## config wlan security wpa gtk-random

To enable the randomization of group temporal keys (GTK) between access points and clients on a WLAN, use the **config wlan security wpa gtk-random** command.

```
config wlan security wpa gtk-random {enable | disable} wlan_id
```

Syntax Description	enable	disable	wlan_id
	Enables the randomization of GTK keys between the access point and clients.	Disables the randomization of GTK keys between the access point and clients.	WLAN identifier between 1 and 512.

Command Default	None
-----------------	------

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** When you enable this command, the clients in the Basic Service Set (BSS) get a unique GTK key. The clients do not receive multicast or broadcast traffic.

The following example shows how to enable the GTK randomization for each client associated on a WLAN:

```
(Cisco Controller) >config wlan security wpa gtk-random enable 3
```

## config wlan security wpa wpa1 disable

To disable WPA1, use the **config wlan security wpa wpa1 disable** command.

**config wlan security wpa wpa1 disable** *wlan\_id*

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable WPA1:

```
(Cisco Controller) >config wlan security wpa wpa1 disable 1
```

## config wlan security wpa wpa1 enable

To enable WPA1, use the **config wlan security wpa wpa1 enable** command.

**config wlan security wpa wpa1 enable** *wlan\_id*

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA1:

```
(Cisco Controller) >config wlan security wpa wpa1 enable 1
```

## config wlan security wpa wpa2 disable

To disable WPA2, use the **config wlan security wpa wpa2 disable** command.

**config wlan security wpa wpa2 disable** *wlan\_id*

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 disable 1
```



## config wlan security wpa wpa2 enable

To enable WPA2, use the **config wlan security wpa wpa2 enable** command.

**config wlan security wpa wpa2 enable** *wlan\_id*

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 enable 1
```

## config wlan security wpa wpa2 cache

To configure caching methods on a WLAN, use the **config wlan security wpa wpa2 cache** command.

```
config wlan security wpa wpa2 cache sticky {enable | disable} wlan_id
```

### Syntax Description

<b>sticky</b>	Configures Sticky Key Caching (SKC) roaming support on the WLAN.
<b>enable</b>	Enables SKC roaming support on the WLAN.
<b>disable</b>	Disables SKC roaming support on the WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

In SKC (Sticky Key caching) also known as PKC (Pro Active Key caching), the client stores each Pairwise Master Key (PMK) ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has a PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs.

The following example shows how to enable SKC roaming support on a WLAN:

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 1
```

## config wlan security wpa wpa2 cache sticky

To configure Sticky PMKID Caching (SKC) on a WLAN, use the **config wlan security wpa wpa2 cache sticky** command.

```
config wlan security wpa wpa2 cache sticky {enable | disable} wlan_id
```

### Syntax Description

<b>enable</b>	Enables SKC on a WLAN.
<b>disable</b>	Disables SKC on a WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512 (inclusive).

### Command Default

Stkcky PMKID Caching is disabled.

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

Beginning in Release 7.2 and later releases, the controller supports Sticky PMKID Caching (SKC). With sticky PMKID caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client. In SKC also known as PKC (Pro Active Key caching), the client stores each Pairwise Master Key (PMK) ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

- You cannot use SKC for large scale deployments as the controller supports SKC only up to eight APs.
- SKC does not work across controllers in a mobility group.
- SKC works only on WPA2-enabled WLANs.
- SKC works only on local mode APs.

The following example shows how to enable Sticky PMKID Caching on WLAN 5:

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 5
```

## config wlan security wpa wpa2 ciphers

To configure WPA2 ciphers and enable or disable Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) data encryption for WPA2, use the **config wlan security wpa wpa2 ciphers** command

```
config wlan security wpa wpa2 ciphers {aes | tkip} {enable | disable} wlan_id
```

### Syntax Description

(Cisco Controller) > <b>aes</b>	Configures AES data encryption for WPA2.
<b>tkip</b>	Configures TKIP data encryption for WPA2.
<b>enable</b>	Enables AES or TKIP data encryption for WPA2.
<b>disable</b>	Disables AES or TKIP data encryption for WPA2.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

### Command Default

AES is enabled by default.

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable AES data encryption for WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1
```

## config wlan sip-cac disassoc-client

To enable client disassociation in case of session initiation protocol (SIP) call admission control (CAC) failure, use the **config wlan sip-cac disassoc-client** command.

```
config wlan sip-cac disassoc-client {enable | disable} wlan_id
```

Syntax Description		
	<b>enable</b>	Enables a client disassociation on a SIP CAC failure.
	<b>disable</b>	Disables a client disassociation on a SIP CAC failure.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

**Command Default** Client disassociation for SIP CAC is disabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a client disassociation on a SIP CAC failure where the WLAN ID is 1:

```
(Cisco Controller) >config wlan sip-cac disassoc-client enable 1
```

## config wlan sip-cac send-486busy

To configure sending session initiation protocol (SIP) 486 busy message if a SIP call admission control (CAC) failure occurs, use the **config wlan sip-cac send-486busy** command:

```
config wlan sip-cac send-486busy {enable | disable} wlan_id
```

Syntax Description	enable	disable	wlan_id
	Enables sending a SIP 486 busy message upon a SIP CAC failure.	Disables sending a SIP 486 busy message upon a SIP CAC failure.	Wireless LAN identifier between 1 and 512.
Command Default	Session initiation protocol is enabled by default.		
Command History	Release	Modification	
	7.6	This command was introduced in a release earlier than Release 7.6.	

The following example shows how to enable sending a SIP 486 busy message upon a SIP CAC failure where the WLAN ID is 1:

```
(Cisco Controller) >config wlan sip-cac send-busy486 enable 1
```

## config wlan static-ip tunneling

To configure static IP client tunneling support on a WLAN, use the **config wlan static-ip tunneling** command.

```
config wlan static-ip tunneling {enable | disable} wlan_id
```

Syntax Description		
<b>tunneling</b>	Configures static IP client tunneling support on a WLAN.	
<b>enable</b>	Enables static IP client tunneling support on a WLAN.	
<b>disable</b>	Disables static IP client tunneling support on a WLAN.	
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable static IP client tunneling support for WLAN ID 3:

```
(Cisco Controller) >config wlan static-ip tunneling enable 34
```

## config wlan session-timeout

To change the timeout of wireless LAN clients, use the **config wlan session-timeout** command.

**config wlan session-timeout** {*wlan\_id* | **foreignAp**} *seconds*

### Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>foreignAp</b>	Specifies third-party access points.
<i>seconds</i>	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

**Note** The range of session timeout depends on the security type:

- Open system: 0-65535 (sec)
- 802.1x: 300-86400 (sec)
- static wep: 0-65535 (sec)
- cranite: 0-65535 (sec)
- fortress: 0-65535 (sec)
- CKIP: 0-65535 (sec)
- open+web auth: 0-65535 (sec)
- web pass-thru: 0-65535 (sec)
- wpa-psk: 0-65535 (sec)
- disable: To disable reauth/session-timeout timers.

### Command Default

None

### Usage Guidelines

For 802.1X client security type, which creates the PMK cache, the maximum session timeout that can be set is 86400 seconds when the session timeout is disabled. For other client security such as open, WebAuth, and PSK for which the PMK cache is not created, the session timeout value is shown as infinite when session timeout is disabled.

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the client timeout to 6000 seconds for WLAN ID 1:

```
(Cisco Controller) >config wlan session-timeout 1 6000
```



## config wlan uapsd compliant client enable

To enable WPA1, use the **config wlan uapsd compliant-client enable** command.



**Note** This was introduced for Ascom non-wmm capable phones and is not applicable for Cisco 792x/9971 IP phones.

**config wlan uapsd compliant-client enable** *wlan-id*

### Syntax Description

*wlan\_id* Wireless LAN identifier between 1 and 512.

### Command Default

None

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA1:

```
(Cisco Controller) >config wlan uapsd compliant-client enable 1
```

Property Type	Property Value	Property Description

## config wlan uapsd compliant-client disable

To disable WPA1, use the **config wlan uapsd compliant-client disable** command.



**Note** This was introduced for Ascom non-wmm capable phones and is not applicable for Cisco 792x/9971 IP phones.

**config wlan uapsd compliant-client disable** *wlan-id*

Syntax Description	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
--------------------	----------------	--

Command Default	None
-----------------	------

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA1:

```
(Cisco Controller) >config wlan uapsd compliant-client disable 1
```

## config wlan user-idle-threshold

To configure the threshold data sent by the client during the idle timeout for client sessions for a WLAN, use the **config wlan user-idle-threshold** command.

**config wlan user-idle-threshold** *bytes wlan\_id*

<b>Syntax Description</b>	<i>bytes</i>	Threshold data sent by the client during the idle timeout for the client session for a WLAN. If the client send traffic less than the defined threshold, the client is removed on timeout. The range is from 0 to 10000000 bytes.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<b>Command Default</b>	The default timeout for threshold data sent by client during the idle timeout is 0 bytes.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the threshold data sent by the client during the idle timeout for client sessions for a WLAN:

```
(Cisco Controller) >config wlan user-idle-threshold 100 1
```

# config wlan usertimeout

To configure the timeout for idle client sessions for a WLAN, use the **config wlan usertimeout** command.

**config wlan usertimeout** *timeout wlan\_id*

## Syntax Description

*timeout* Timeout for idle client sessions for a WLAN. If the client sends traffic less than the threshold, the client is removed on timeout. The range is from 15 to 100000 seconds.

*wlan\_id* Wireless LAN identifier between 1 and 512.

## Command Default

The default client session idle timeout is 300 seconds.

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

## Usage Guidelines

The timeout value that you configure here overrides the global timeout that you define using the command **config network usertimeout**.

The following example shows how to configure the idle client sessions for a WLAN:

```
(Cisco Controller) >config wlan usertimeout 100 1
```

## config wlan webauth-exclude

To release the guest user IP address when the web authentication policy time expires and exclude the guest user from acquiring an IP address for three minutes, use the **config wlan webauth-exclude** command.

```
config wlan webauth-exclude wlan_id { enable | disable }
```

Syntax Description		
	<i>wlan_id</i>	Wireless LAN identifier (1 to 512).
	<b>enable</b>	Enables web authentication exclusion.
	<b>disable</b>	Disables web authentication exclusion.

**Command Default** Disabled.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

You can use this command for guest WLANs that are configured with web authentication.

This command is applicable when you configure the internal DHCP scope on the controller.

By default, when the web authentication timer expires for a guest user, the guest user can immediately reassociate with the same IP address before another guest user can acquire the IP address. If there are many guest users or limited IP address in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user's IP address is released when the web authentication policy time expires and the guest user is excluded from acquiring an IP address for three minutes. The IP address is available for another guest user to use. After three minutes, the excluded guest user can reassociate and acquire an IP address, if available.

The following example shows how to enable the web authentication exclusion for WLAN ID 5:

```
(Cisco Controller) >config wlan webauth-exclude 5 enable
```

# config wlan wifidirect

To configure Wi-Fi Direct Client Policy on a WLAN, use the **config wlan wifidirect** command.

**config wlan wifidirect** { **allow** | **disable** | **not-allow** | **xconnect-not-allow** } *wlan\_id*

## Syntax Description

<b>allow</b>	Allows Wi-Fi Direct clients to associate with the WLAN
<b>disable</b>	Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate
<b>not-allow</b>	Disallows the Wi-Fi Direct clients from associating with the WLAN
<b>xconnect-not-allow</b>	Enables AP to allow a client with the Wi-Fi Direct option enabled to associate, but the client (if it works according to the Wi-Fi standards) will refrain from setting up a peer-to-peer connection
<i>wlan_id</i>	Wireless LAN identifier (1 to 16).

## Command Default

None

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to allow Wi-Fi Direct Client Policy on WLAN ID 1:

```
(Cisco Controller) >config wlan wifidirect allow 1
```

## config wlan wmm

To configure Wi-Fi Multimedia (WMM) mode on a wireless LAN, use the **config wlan wmm** command.

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

Syntax Description	allow	Allows WMM on the wireless LAN.
	disable	Disables WMM on the wireless LAN.
	require	Specifies that clients use WMM on the specified wireless LAN.
	wlan_id	Wireless LAN identifier (1 to 512).
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

### Usage Guidelines

When the controller is in Layer 2 mode and WMM is enabled, you must put the access points on a trunk port in order to allow them to join the controller.

The following example shows how to configure wireless LAN ID 1 to allow WMM:

```
(Cisco Controller) >config wlan wmm allow 1
```

The following example shows how to configure wireless LAN ID 1 to specify that clients use WMM:

```
(Cisco Controller) >config wlan wmm require 1
```

# config Commands

This section lists the **config** commands to configure WLANs.



## debug 11v all

To configure the 802.11v debug options, use the **debug 11v all** command.

**debug 11v all** { **enable** | **disable** }

Syntax Description	
<b>enable</b>	Enables all the debug.
<b>disable</b>	Disables all the debug.

Command Default	None
-----------------	------

Command History	Release	Modification
	8.1	This command was introduced.

The following example shows how to enable all the debug:

```
(Cisco Controller) >debug 11v all enable
```

## debug 11v detail

To configure the 802.11v debug details, use the **debug 11v detail** command.

**debug 11v detail** { **enable** | **disable** }

Syntax Description	
<b>enable</b>	Enables debug details.
<b>disable</b>	Disables debug details.

Command Default	
	None

Command History	Release	Modification
	8.1	This command was introduced.

The following example shows how to enable 802.11v debug details:

```
(Cisco Controller) >debug 11v detail enable
```

## debug 11v error

To configure the 802.11v error debug options, use the **debug 11v errors** command.

**debug 11v errors** { **enable** | **disable** }

<b>Syntax Description</b>	<b>enable</b> Enables error debug.
	<b>disable</b> Disables error debug.

<b>Command Default</b>	None
------------------------	------

<b>Command History</b>	<b>Release</b> <b>Modification</b>
	8.1 This command was introduced.

The following example shows how to enable 802.11v error debug:

```
(Cisco Controller) >debug 11v error enable
```

## debug 11w-pmf

To configure the debugging of 802.11w, use the **debug 11w-pmf** command.

**debug 11w-pmf** { **all** | **events** | **keys** } { **enable** | **disable** }

### Syntax Description

<b>all</b>	Configures the debugging of all 802.11w messages.
<b>keys</b>	Configures the debugging of 802.11w keys.
<b>events</b>	Configures the debugging of 802.11w events.
<b>enable</b>	Enables the debugging of 802.1w options.
<b>disable</b>	Disables the debugging of 802.1w options.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of 802.11w keys:

```
(Cisco Controller) >debug 11w-pmf keys enable
```

# debug call-control

To configure the debugging of the SIP call control settings, use the **debug call-control** command.

**debug call-control** {all | event} {enable | disable}

Syntax Description	all	event	enable	disable
	Configures the debugging options for all SIP call control messages.	Configures the debugging options for SIP call control events.	Enables the debugging of SIP call control messages or events.	Disables the debugging of SIP call control messages or events.
Command Default	Disabled.			
Command History	Release	Modification		
	7.6	This command was introduced in a release earlier than Release 7.6.		

The following example shows how to enable the debugging of all SIP call control messages:

```
(Cisco Controller) >debug call-control all enable
```

## debug ccxdia

To configure debugging of Cisco Compatible Extensions (CCX) diagnostic options, use the **debug ccxdia** command.

**debug ccxdia** {all | error | event | packet} {enable | disable}

### Syntax Description

<b>all</b>	Configures debugging of all the CCX S69 messages.
<b>error</b>	Configures debugging of the CCX S69 errors.
<b>event</b>	Configures debugging of the CCX S69 events.
<b>packet</b>	Configures debugging of the CCX S69 packets.
<b>enable</b>	Enables debugging of the CCX S69 options.
<b>disable</b>	Disables debugging of the CCX S69 options.

### Command Default

None

### Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable CCX S69 packets debugging:

```
(Cisco Controller) >debug ccxdia packets enable
```

## debug ccxrm

To configure debugging of the CCX Cisco Client eXtension (CCX) Radio Management (RM), use the **debug ccxrm** command.

```
debug ccxrm {all | detail | error | location-calibration | message | packet | warning}
{enable | disable}
```

Syntax Description	all	Configures debugging of all CCX RM messages.
	<b>detail</b>	Configures detailed debugging of CCX RM.
	<b>error</b>	Configures debugging of the CCX RM errors.
	<b>location-calibration</b>	Configures debugging of the CCX RM location calibration.
	<b>message</b>	Configures debugging of CCX RM messages.
	<b>packet</b>	Configures debugging of the CCX RM packets.
	<b>warning</b>	Configures debugging of the CCX RM warnings.
	<b>enable</b>	Enables debugging of the CCX RM options.
	<b>disable</b>	Disables debugging of the CCX RM options.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable CCX RM debugging:

```
(Cisco Controller) > debug ccxrm all enable
```

## debug ccxs69

To configure debugging of CCX S69 tasks, use the **debug ccxs69** command.

**debug ccxs69** {all | error | event} {enable | disable}

Syntax Description		
<b>all</b>	Configures debugging of all the CCX S69 messages.	
<b>error</b>	Configures debugging of the CCX S69 errors.	
<b>event</b>	Configures debugging of the CCX S69 events.	
<b>enable</b>	Enables debugging of the CCX S69 options.	
<b>disable</b>	Disables debugging of the CCX S69 options.	

Command Default	
	None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable CCX S69 debugging:

```
(Cisco Controller) >debug ccxs69 all enable
```



# debug client

To configure the debugging of a passive client that is associated correctly with the access point, use the **debug client** command.

**debug client** *mac\_address*

<b>Syntax Description</b>	<i>mac_address</i>	MAC address of the client.
---------------------------	--------------------	----------------------------

<b>Command Default</b>	None
------------------------	------

The following example shows how to debug a passive client with MAC address 00:0d:28:f4:c0:45:

```
(Cisco Controller) >debug client 00:0d:28:f4:c0:45
```

# debug dhcp

To configure the debugging of DHCP, use the **debug dhcp** command.

**debug dhcp** {message | packet} {enable | disable}

## Syntax Description

<b>message</b>	Configures the debugging of DHCP error messages.
<b>packet</b>	Configures the debugging of DHCP packets.
<b>enable</b>	Enables the debugging DHCP messages or packets.
<b>disable</b>	Disables the debugging of DHCP messages or packets.

## Command Default

None

The following example shows how to enable the debugging of DHCP messages:

```
(Cisco Controller) >debug dhcp message enable
```

## debug dhcp service-port

To enable or disable debugging of the Dynamic Host Configuration Protocol (DHCP) packets on the service port, use the **debug dhcp service-port** command.

**debug dhcp service-port** {enable | disable}

<b>Syntax Description</b>	<b>enable</b>	Enables the debugging of DHCP packets on the service port.
	<b>disable</b>	Disables the debugging of DHCP packets on the service port.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of DHCP packets on a service port:

```
(Cisco Controller) >debug dhcp service-port enable
```

# debug ft

To configure debugging of 802.11r, use the **debug ft** command.

**debug ft** { **events** | **keys** } { **enable** | **disable** }

## Syntax Description

<b>events</b>	Configures debugging of the 802.11r events.
<b>keys</b>	Configures debugging of the 802.11r keys.
<b>enable</b>	Enables debugging of the 802.11r options.
<b>disable</b>	Disables debugging of the 802.11r options.

## Command Default

None

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable 802.11r debugging:

```
(Cisco Controller) >debug ft events enable
```

# debug hotspot

To configure debugging of HotSpot events or packets, use the **debug hotspot** command.

**debug hotspot** { **events** | **packets** } { **enable** | **disable** } { **enable** | **disable** }

Syntax Description	events	Configures debugging of HotSpot events.
	packets	Configures debugging of HotSpot packets.
	enable	Enables the debugging of HotSpot options.
	disable	Disables the debugging of HotSpot options.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable debugging of hotspot events:

```
(Cisco Controller) >debug hotspot events enable
```

# debug ipv6

To configure debugging of IPv6 options, use the **debug ipv6** command.

**debug ipv6** {**all** | **bt** | **classifier** | **errors** | **events** | **filter** | **fsm** | **gleaner** | **hwapi** | **memory** | **ndsuppress** | **parser** | **policy** | **ra\_throttler** | **switcher**} {**enable** | **disable**}

## Syntax Description

<b>all</b>	Configures debugging of all the IPv6 information.
<b>bt</b>	Configures debugging of the IPv6 neighbor binding table.
<b>classifier</b>	Configures debugging of the IPv6 packet classifiers.
<b>errors</b>	Configures debugging of the IPv6 errors.
<b>events</b>	Configures debugging of the IPv6 events.
<b>filter</b>	Configures filters for the IPv6 debugs.
<b>fsm</b>	Configures debugging of the IPv6 finite state machine (FSM).
<b>gleaner</b>	Configures debugging of the IPv6 gleaner. Learning of entries is called gleaning.
<b>hwapi</b>	Configures debugging of the IPv6 hardware APIs.
<b>memory</b>	Configures debugging of the IPv6 binding table memory usage.
<b>ndsuppress</b>	Configures debugging of the suppressed IPv6 neighbor discoveries.
<b>parser</b>	Configures debugging of the IPv6 parser.
<b>policy</b>	Configures debugging of the IPv6 policies.
<b>ra_throttler</b>	Configures debugging of the IPv6 router advertising throttler.
<b>switcher</b>	Configures debugging of the IPv6 switcher.
<b>enable</b>	Enables debugging of the IPv6 options.
<b>disable</b>	Disables debugging of the IPv6 options.

## Command Default

None

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of IPv6 policies:

```
(Cisco Controller) >debug ipv6 policy enable
```

# debug profiling

To configure the debugging of client profiling, use the **debug profiling** command.

**debug profiling** { **enable** | **disable** }

---

**Syntax Description**

**enable** Enables the debugging of client profiling (HTTP and DHCP profiling).

**disable** Disables the debugging of client profiling (HTTP and DHCP profiling).

---

**Command Default**

Disabled.

---

**Command History**

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to enable the debugging of client profiling:

```
(Cisco Controller) >debug profiling enable
```

# debug wcp

To configure the debugging of WLAN Control Protocol (WCP), use the **debug wcp** command.

**debug wcp** { **events** | **packet** } { **enable** | **disable** }

Syntax Description		
<b>events</b>	Configures the debugging of WCP events.	
<b>packet</b>	Configures the debugging of WCP packets.	
<b>enable</b>	Enables the debugging of WCP settings.	
<b>disable</b>	Disables the debugging of WCP settings.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of WCP settings:

```
(Cisco Controller) >debug wcp packet enable
```



# show advanced hotspot

To display the advanced HotSpot parameters, use the **show advanced hotspot** command.

## show advanced hotspot

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Default</b>	None
------------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the advanced HotSpot parameters:

```
(Cisco Controller) >show advanced hotspot
ANQP 4-way state..... Disabled
GARP Broadcast state: ..... Enabled
GAS request rate limit ..... Disabled
ANQP comeback delay in TUs(TU=1024usec)..... 50
```

### Related Topics

[show wlan](#), on page 287

[debug hotspot](#), on page 237

[config wlan apgroup](#), on page 87

[config wlan security wpa gtk-random](#), on page 205

[config wlan hotspot](#), on page 113

## show avc statistics wlan

To display the Application Visibility and Control (AVC) statistics of a WLAN, use the **show avc statistics wlan** command.

**show avc statistics wlan** *wlan\_id* {**application** *application\_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**] }

Syntax Description		
<b>wlan_id</b>		WLAN identifier from 1 to 512.
<b>application</b>		Displays AVC statistics for an application.
<b>application_name</b>		Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
<b>top-app-groups</b>		Displays AVC statistics for top application groups.
<b>upstream</b>		(Optional) Displays statistics of top upstream applications.
<b>downstream</b>		(Optional) Displays statistics of top downstream applications.
<b>top-apps</b>		Displays AVC statistics for top applications.

**Command Default** None

Command History	Release	Modification
	7.4	This command was introduced.

The following is a sample output of the **show avc statistics** command.

```
(Cisco Controller) >show avc statistics wlan 1
```

Application-Name (Up/Down)	Packets (n secs)	Bytes (n secs)	Avg Pkt Size	Packets (Total)	Bytes (Total)
=====	=====	=====	=====	=====	=====
unclassified	(U) 191464	208627	1	92208613	11138796586
	(D) 63427	53440610	842	16295621	9657054635
ftp	(U) 805	72880	90	172939	11206202
	(D) 911	58143	63	190900	17418653
http	(U) 264904	12508288	47	27493945	2837672192
	(D) 319894	436915253	1365	29850934	36817587924
gre	(U) 0	0	0	10158872	10402684928
	(D) 0	0	0	0	0
icmp	(U) 1	40	40	323	98476
	(D) 7262	4034576	555	2888266	1605133372
ipinip	(U) 62565	64066560	1024	11992305	12280120320
	(D) 0	0	0	0	0
imap	(U) 1430	16798	11	305161	3795766
	(D) 1555	576371	370	332290	125799465
irc	(U) 9	74	8	1736	9133
	(D) 11	371	33	1972	173381
nntp	(U) 22	158	7	1705	9612
	(D) 22	372	16	2047	214391

The following is a sample output of the **show avc statistics wlan** command.

```
(Cisco Controller) >show avc statistics wlan 1 application ftp
```

Description	Upstream	Downstream
=====	=====	=====
Number of Packtes(n secs)	0	0
Number of Bytes(n secs)	0	0
Average Packet size(n secs)	0	0
Total Number of Packtes	32459	64888
Total Number of Bytes	274	94673983

### Related Topics

[config wlan avc](#), on page 86

# show call-control ap



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

To see the metrics for successful calls or the traps generated for failed calls, use the **show call-control ap** command.

```
show call-control ap {802.11a | 802.11b} cisco_ap {metrics | traps}
```

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

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** To aid in troubleshooting, the output of this command shows an error code for any failed calls. This table explains the possible error codes for failed calls.

**Table 2: Error Codes for Failed VoIP Calls**

Error Code	Integer	Description
1	unknown	Unknown error.
400	badRequest	The request could not be understood because of malformed syntax.
401	unauthorized	The request requires user authentication.
402	paymentRequired	Reserved for future use.
403	forbidden	The server understood the request but refuses to fulfill it.
404	notFound	The server has information that the user does not exist at the domain specified in the Request-URI.

Error Code	Integer	Description
405	methodNotAllowed	The method specified in the Request-Line is understood but not allowed for the address identified by the Request-URI.
406	notAcceptable	The resource identified by the request is only capable of generating response entities with content characteristics that are not acceptable according to the Accept header field sent in the request.
407	proxyAuthenticationRequired	The client must first authenticate with the proxy.
408	requestTimeout	The server could not produce a response within a suitable amount of time.
409	conflict	The request could not be completed due to a conflict with the current state of the resource.
410	gone	The requested resource is no longer available at the server, and no forwarding address is known.
411	lengthRequired	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
413	requestEntityTooLarge	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
414	requestURITooLarge	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415	unsupportedMediaType	The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method.

Error Code	Integer	Description
420	badExtension	The server did not understand the protocol extension specified in a Proxy-Require or Require header field.
480	temporarilyNotAvailable	The callee's end system was contacted successfully, but the callee is currently unavailable.
481	callLegDoesNotExist	The UAS received a request that does not match any existing dialog or transaction.
482	loopDetected	The server has detected a loop.
483	tooManyHops	The server received a request that contains a Max-Forwards header field with the value zero.
484	addressIncomplete	The server received a request with a Request-URI that was incomplete.
485	ambiguous	The Request-URI was ambiguous.
486	busy	The callee's end system was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system.
500	internalServerError	The server encountered an unexpected condition that prevented it from fulfilling the request.
501	notImplemented	The server does not support the functionality required to fulfill the request.
502	badGateway	The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
503	serviceUnavailable	The server is temporarily unable to process the request because of a temporary overloading or maintenance of the server.

Error Code	Integer	Description
504	serverTimeout	The server did not receive a timely response from an external server it accessed in attempting to process the request.
505	versionNotSupported	The server does not support or refuses to support the SIP protocol version that was used in the request.
600	busyEverywhere	The callee's end system was contacted successfully, but the callee is busy or does not want to take the call at this time.
603	decline	The callee's machine was contacted successfully, but the user does not want to or cannot participate.
604	doesNotExistAnywhere	The server has information that the user indicated in the Request-URI does not exist anywhere.
606	notAcceptable	The user's agent was contacted successfully, but some aspects of the session description (such as the requested media, bandwidth, or addressing style) were not acceptable.

The following is a sample output of the **show call-controller ap** command that displays successful calls generated for an access point:

```
(Cisco Controller) >show call-control ap 802.11a Cisco_AP metrics
Total Call Duration in Seconds..... 120
Number of Calls..... 10
Number of calls for given client is..... 1
```

The following is a sample output of the **show call-control ap** command that displays metrics of traps generated for an AP.

```
(Cisco Controller) >show call-control ap 802.11a Cisco_AP traps
Number of traps sent in one min..... 2
Last SIP error code..... 404
Last sent trap timestamp..... Jun 20 10:05:06
```

## show call-control client

To see call information for a call-aware client when Voice-over-IP (VoIP) snooping is enabled and the call is active, use the **show call-control client** command

**show call-control client callInfo** *client\_MAC\_address*

<b>Syntax Description</b>	<b>callInfo</b>	Specifies the call-control information.
	<i>client_MAC_address</i>	Client MAC address.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example is a sample output of the **show call-controller client** command:

```
(Cisco Controller) > show call-control client callInfo 10.10.10.10.10
Uplink IP/port..... 0.0.0.0 / 0
Downlink IP/port..... 9.47.96.107 / 5006
UP..... 6
Calling Party..... sip:1021
Called Party..... sip:1000
Call ID..... 38423970c3fca477
Call on hold: ..... FALSE
Number of calls for given client is..... 1
```



## show client ccx client-capability

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

**show client ccx client-capability** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	This command displays the client's available capabilities, not the current settings for the capabilities.	

The following is a sample output of the **show client ccx client-capability** command:

```
(Cisco Controller) >show client ccx client-capability 00:40:96:a8:f7:98
Service Capability..... Voice, Streaming(uni-directional)
Video, Interactive(bi-directional) Video
Radio Type..... DSSS OFDM(802.11a) HRDSSS(802.11b)
ERP(802.11g)
Radio Type..... DSSS
Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode..... Automatic
Rate List(MB)..... 1.0 2.0
Radio Type..... HRDSSS(802.11b)
Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode..... Automatic
Rate List(MB)..... 5.5 11.0
Radio Type..... ERP(802.11g)
Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode..... Automatic
Rate List(MB)..... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Are you sure you want to start? (y/N)y Are you sure you want to start? (y/N)
```

## show client ccx frame-data

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

**show client ccx frame-data** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx frame-data** command:

```
(Cisco Controller) >show client ccx frame-data
xx:xx:xx:xx:xx:xx
```

## show client ccx last-response-status

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

**show client ccx last-response-status** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx last-response-status** command:

```
(Cisco Controller) >show client ccx last-response-status
Test Status ..... Success
Response Dialog Token..... 87
Response Status..... Successful
Response Test Type..... 802.1x Authentication Test
Response Time..... 3476 seconds since system boot
```

## show client ccx last-test-status

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

**show client ccx last-test-status** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx last-test-status** command:

```
(Cisco Controller) >show client ccx last-test-status

Test Type ..... Gateway Ping Test
Test Status ..... Pending/Success/Timeout
Dialog Token ..... 15
Timeout ..... 15000 ms
Request Time ..... 1329 seconds since system boot
```

# show client ccx log-response

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

**show client ccx log-response** {roam | rsna | syslog} *client\_mac\_address*

Syntax Description	roam	(Optional) Displays the CCX client roaming log response.
	rsna	(Optional) Displays the CCX client RSNA log response.
	syslog	(Optional) Displays the CCX client system log response.
	<i>client_mac_address</i>	Inventory for the specified access point.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx log-response syslog** command:

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

The following example shows how to display the client roaming log response:

```
(Cisco Controller) >show client ccx log-response roam 00:40:96:a8:f7:98
Thu Jun 22 11:55:14 2007      Roaming Response LogID=20: Status=Successful
Event Timestamp=0d 00h 00m 13s 322396us      Source BSSID=00:40:96:a8:f7:98
Target BSSID=00:0b:85:23:26:70,      Transition Time=100 (ms)
Transition Reason: Normal roam, poor link      Transition Result: Success
Thu Jun 22 11:55:14 2007      Roaming Response LogID=133: Status=Successful
Event Timestamp=0d 00h 00m 16s 599006us      Source BSSID=00:0b:85:81:06:c2
Target BSSID=00:0b:85:81:06:c2,      Transition Time=3235 (ms)
Transition Reason: Normal roam, poor link      Transition Result: Success
Thu Jun 22 18:28:48 2007      Roaming Response LogID=133: Status=Successful
Event Timestamp=0d 00h 00m 08s 815477us      Source BSSID=00:0b:85:81:06:c2
Target BSSID=00:0b:85:81:06:d2,      Transition Time=3281 (ms)
Transition Reason: First association to WLAN      Transition Result: Success
```

## show client ccx manufacturer-info

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

**show client ccx manufacturer-info** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx manufacturer-info** command:

```
(Cisco Controller) >show client ccx manufacturer-info 00:40:96:a8:f7:98
Manufacturer OUI ..... 00:40:96
Manufacturer ID ..... Cisco
Manufacturer Model ..... Cisco Aironet 802.11a/b/g Wireless Adapter
Manufacturer Serial ..... FOC1046N3SX
Mac Address ..... 00:40:96:b2:8d:5e
Radio Type ..... DSSS OFDM(802.11a) HRDSSS(802.11b)
    ERP(802.11g)
Antenna Type ..... Omni-directional diversity
Antenna Gain ..... 2 dBi
Rx Sensitivity:
Radio Type ..... DSSS
Rx Sensitivity ..... Rate:1.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ..... Rate:2.0 Mbps, MinRssi:-95, MaxRssi:-30
Radio Type ..... HRDSSS(802.11b)
Rx Sensitivity ..... Rate:5.5 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ..... Rate:11.0 Mbps, MinRssi:-95, MaxRssi:-30
Radio Type ..... ERP(802.11g)
Rx Sensitivity ..... Rate:6.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ..... Rate:9.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ..... Rate:12.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ..... Rate:18.0 Mbps, MinRssi:-95, MaxRssi:-30
```



# show client ccx profiles

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

**show client ccx profiles** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx profiles** command:

```
(Cisco Controller) >show client ccx profiles 00:40:96:15:21:ac
Number of Profiles ..... 1
Current Profile ..... 1
Profile ID ..... 1
Profile Name ..... wifiEAP
SSID ..... wifiEAP
Security Parameters [EAP Method, Credential]..... EAP-TLS, Host OS Login Credentials
Auth Method ..... EAP
Key Management ..... WPA2+CCKM
Encryption ..... AES-CCMP
Power Save Mode ..... Constantly Awake
Radio Configuration:
Radio Type..... DSSS
  Preamble Type..... Long preamble
  CCA Method..... Energy Detect + Carrier
Detect/Correlation
Data Retries..... 6
Fragment Threshold..... 2342
Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode..... Automatic
Rate List (MB)..... 1.0 2.0
Radio Type..... HRDSSS(802.11b)
  Preamble Type..... Long preamble
  CCA Method..... Energy Detect + Carrier
Detect/Correlation
Data Retries..... 6
Fragment Threshold..... 2342
Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode..... Automatic
Rate List (MB)..... 5.5 11.0
Radio Type..... ERP(802.11g)
  Preamble Type..... Long preamble
  CCA Method..... Energy Detect + Carrier
Detect/Correlation
Data Retries..... 6
Fragment Threshold..... 2342
Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode..... Automatic
Rate List (MB)..... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Radio Type..... OFDM(802.11a)
  Preamble Type..... Long preamble
  CCA Method..... Energy Detect + Carrier
```



```
Detect/Correlation
Data Retries..... 6
Fragment Threshold..... 2342
Radio Channels..... 36 40 44 48 52 56 60 64 149 153 157 161
165
Tx Power Mode..... Automatic
Rate List (MB)..... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
```

## show client ccx results

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

**show client ccx results** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	MAC address of the client.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx results** command:

```
(Cisco Controller) >show client ccx results xx.xx.xx.xx
dot1x Complete..... Success
EAP Method..... *1,Host OS Login Credentials
dot1x Status..... 255
```

## show client ccx rm

To display Cisco Client eXtension (CCX) client radio management report information, use the **show client ccx rm** command.

```
show client ccx rm client_MAC {status | {report {chan-load | noise-hist | frame | beacon | pathloss } } }
```

Syntax Description		
<i>client_MAC</i>	Client MAC address.	
<b>status</b>	Displays the client CCX radio management status information.	
<b>report</b>	Displays the client CCX radio management report.	
<b>chan-load</b>	Displays radio management channel load reports.	
<b>noise-hist</b>	Displays radio management noise histogram reports.	
<b>beacon</b>	Displays radio management beacon load reports.	
<b>frame</b>	Displays radio management frame reports.	
<b>pathloss</b>	Displays radio management path loss reports.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

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

```
(Cisco Controller) >show client ccx rm 00:40:96:15:21:ac status

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

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

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

Channel Load Report
Client Mac Address..... 00:40:96:ae:53:bc
Timestamp..... 788751121
Incapable Flag..... On
Refused Flag..... On
Chan CCA Busy Fraction
-----
```

```
1 194
2 86
3 103
4 0
5 178
6 82
7 103
8 95
9 13
10 222
11 75
```

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

```
(Cisco Controller) >show client ccx rm 00:40:96:15:21:ac report noise-hist
```

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

## show client ccx stats-report

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

**show client ccx stats-report** *client\_mac\_address*

<b>Syntax Description</b>	<i>client_mac_address</i>	Client MAC address.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx stats-report** command:

```
(Cisco Controller) > show client ccx stats-report 00:0c:41:07:33:a6
Measurement duration = 1
dot11TransmittedFragmentCount          = 1
dot11MulticastTransmittedFrameCount    = 2
dot11FailedCount                        = 3
dot11RetryCount                         = 4
dot11MultipleRetryCount                 = 5
dot11FrameDuplicateCount                = 6
dot11RTSSuccessCount                   = 7
dot11RTSFailureCount                   = 8
dot11ACKFailureCount                   = 9
dot11ReceivedFragmentCount             = 10
dot11MulticastReceivedFrameCount       = 11
dot11FCSErrorCount                     = 12
dot11TransmittedFrameCount             = 13
```

# show client detail

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

**show client detail** *mac\_address*

<b>Syntax Description</b>	<i>mac_address</i>	Client MAC address.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	The <b>show client ap</b> command may list the status of automatically disabled clients. Use the <b>show exclusionlist</b> command to display clients on the exclusion list.	

The following example shows how to display the client detailed information:

```
(Cisco Controller) >show client detail 00:0c:41:07:33:a6
Policy Manager State.....POSTURE_REQD
Policy Manager Rule Created.....Yes
Client MAC Address..... 00:16:36:40:ac:58
Client Username..... N/A
Client State..... Associated
Client NAC OOB State..... QUARANTINE
Guest LAN Id..... 1
IP Address..... Unknown
Session Timeout..... 0
QoS Level..... Platinum
802.1P Priority Tag..... disabled
KTS CAC Capability..... Yes
WMM Support..... Enabled
Power Save..... ON
Diff Serv Code Point (DSPC)..... disabled
Mobility State..... Local
Internal Mobility State..... apfMsMmInitial
Security Policy Completed..... No
Policy Manager State..... WEBAUTH_REQD
Policy Manager Rule Created..... Yes
NPU Fast Fast Notified..... Yes
Last Policy Manager State..... WEBAUTH_REQD
Client Entry Create Time..... 460 seconds
Interface..... wired-guest
FlexConnect Authentication..... Local
FlexConnect Data Switching..... Local
VLAN..... 236
Quarantine VLAN..... 0
Client Statistics:
  Number of Bytes Received..... 66806
    Number of Data Bytes Received..... 160783
    Number of Realtime Bytes Received..... 160783
  Number of Data Bytes Sent..... 23436
  Number of Realtime Bytes Sent..... 23436
  Number of Data Packets Received..... 592
  Number of Realtime Packets Received..... 592
```

```
Number of Data Packets Sent..... 131
Number of Realtime Packets Sent..... 131
Number of Interim-Update Sent..... 0
Number of EAP Id Request Msg Timeouts..... 0
Number of EAP Request Msg Timeouts..... 0
Number of EAP Key Msg Timeouts..... 0
Number of Data Retries..... 0
Number of RTS Retries..... 0
Number of Duplicate Received Packets..... 3
Number of Decrypt Failed Packets..... 0
Number of Mic Failed Packets..... 0
Number of Mic Missing Packets..... 0
Number of RA Packets Dropped..... 6
Number of Policy Errors..... 0
Radio Signal Strength Indicator..... -50 dBm
Signal to Noise Ratio..... 43 dB
...
```

# show client location-calibration summary

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

## show client location-calibration summary

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the location calibration summary information:

```
(Cisco Controller) >show client location-calibration summary
MAC Address Interval
-----
10:10:10:10:10:10 60
21:21:21:21:21:21 45
```



# show client probing

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

## **show client probing**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to display the number of probing clients:

```
(Cisco Controller) >show client probing
Number of Probing Clients..... 0
```

## show client roam-history

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

**show client roam-history** *mac\_address*

<b>Syntax Description</b>	<i>mac_address</i>	Client MAC address.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client roam-history** command:

```
(Cisco Controller) > show client roam-history 00:14:6c:0a:57:77
```

# show client summary

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

**show client summary** [*ssid / ip / username / devicetype*]

## Syntax Description

This command has no arguments or keywords up to Release 7.4.

## Syntax Description

*ssid / ip / username / devicetype*

(Optional) Displays active clients selective details on any of the following parameters or all the parameters in any order:

- SSID
- IP addresss
- Username
- Device type (such as Samsung-Device or WindowsXP-Workstation)

## Command Default

None

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

## Usage Guidelines

Use **show client ap** command to list the status of automatically disabled clients. Use the **show exclusionlist** command to display clients on the exclusion list.

The following example shows how to display a summary of the active clients:

```
(Cisco Controller) > show client summary
Number of Clients..... 24
Number of PMIPv6 Clients..... 200
MAC Address      AP Name      Status      WLAN/GLAN/RLAN Auth Protocol      Port
Wired  PMIPv6
-----  -----
00:00:15:01:00:01 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a      13
  No      Yes
00:00:15:01:00:02 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a      13
  No      No
00:00:15:01:00:03 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a      13
  No      Yes
00:00:15:01:00:04 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a      13
  No      No
```

The following example shows how to display all clients that are WindowsXP-Workstation device type:

```
(Cisco Controller) >show client summary WindowsXP-Workstation
```

show client summary

```
Number of Clients in WLAN..... 0
MAC Address      AP Name      Status      Auth Protocol      Port Wired Mobility Role
-----
Number of Clients with requested device type..... 0
```

# show client wlan

To display the summary of clients associated with a WLAN, use the **show client wlan** command.

**show client wlan** *wlan\_id* [**devicetype** *device*]

<b>Syntax Description</b>	<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
	<b>devicetype</b>	(Optional) Displays all clients with the specified device type.
	<i>device</i>	Device type. For example, Samsung-Device or WindowsXP-Workstation.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following are sample outputs of the **show client wlan** command:

```
(Cisco Controller) > show client wlan 1
```

```
Number of Clients in WLAN..... 0
```

```
(Cisco Controller) > show client devicetype WindowsXP-Workstation
```

```
Number of Clients in WLAN..... 0
```

```
MAC Address      AP Name      Status      Auth Protocol      Port Wired Mobility Role
-----
```

```
Number of Clients with requested device type..... 0
```

# show dhcp

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

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

Syntax Description	leases	Displays allocated DHCP leases.
	<b>summary</b>	Displays DHCP summary information.
	<i>scope</i>	Name of a scope to display the DHCP information for that scope.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the allocated DHCP leases:

```
(Cisco Controller) >show dhcp leases
No leases allocated.
```

The following example shows how to display the DHCP summary information:

```
(Cisco Controller) >show dhcp summary
Scope Name      Enabled      Address Range
003             No          0.0.0.0 -> 0.0.0.0
```

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

```
(Cisco Controller) >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
```

# show dhcp proxy

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

## **show dhcp proxy**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to display the status of DHCP proxy information:

```
(Cisco Controller) >show dhcp proxy
```

```
DHCP Proxy Behavior: enabled
```

# show dhcp timeout

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

## show dhcp timeout

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to display the DHCP timeout value:

```
(Cisco Controller) >show dhcp timeout
DHCP Timeout (seconds)..... 10
```



## show guest-lan

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

**show guest-lan** *guest\_lan\_id*

<b>Syntax Description</b>	<i>guest_lan_id</i>	ID of the selected wired guest LAN.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

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

The following is a sample output of the **show guest-lan** *guest\_lan\_id* command:

```
(Cisco Controller) >show guest-lan 2
Guest LAN Identifier..... 1
Profile Name..... guestlan
Network Name (SSID)..... guestlan
Status..... Enabled
AAA Policy Override..... Disabled
Number of Active Clients..... 1
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... wired
Ingress Interface..... wired-guest
WLAN ACL..... unconfigured
DHCP Server..... 10.20.236.90
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
Security
  Web Based Authentication..... Enabled
  ACL..... Unconfigured
  Web-Passthrough..... Disabled
  Conditional Web Redirect..... Disabled
  Auto Anchor..... Disabled
Mobility Anchor List
GLAN ID IP Address Status
```

# show ipv6 acl

To display the IPv6 access control lists (ACLs) that are configured on the controller, use the **show ipv6 acl** command.

**show ipv6 acl detailed** { *acl\_name* | **summary** }

<b>Syntax Description</b>	<i>acl_name</i>	IPv6 ACL name. The name can be up to 32 alphanumeric characters.
	<b>detailed</b>	Displays detailed information about a specific ACL.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

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

```
(Cisco Controller) >show ipv6 acl detailed acl6
Rule Index..... 1
Direction..... Any
IPv6 source prefix..... ::/0
IPv6 destination prefix..... ::/0
Protocol..... Any
Source Port Range..... 0-65535
Destination Port Range..... 0-65535
DSCP..... Any
Flow label..... 0
Action..... Permit
Counter..... 0
Deny Counter..... 0
```

## show ipv6 neighbor-binding

To display the IPv6 neighbor binding data that are configured on the controller, use the **show ipv6 neighbor-binding** command.

```
show ipv6 neighbor-binding {capture-policy | counters | detailed {mac mac_address | port
port_number | vlanvlan_id} | features | policies | ra-throttle {statistics vlan_id | routers vlan_id}
| summary}
```

Syntax Description		
<b>capture-policy</b>	Displays IPv6 next-hop message capture policies.	
<b>counters</b>	Displays IPv6 next-hop counters (Bridging mode only).	
<b>detailed</b>	Displays the IPv6 neighbor binding table.	
<b>mac</b>	Displays the IPv6 binding table entries for a specific MAC address.	
<i>mac_address</i>	Displays the IPv6 binding table entries for a specific MAC address.	
<b>port</b>	Displays the IPv6 binding table entries for a specific port.	
<i>port_number</i>	Port Number. You can enter ap for an access point or LAG for a LAG port.	
<b>vlan</b>	Displays the IPv6 neighbor binding table entries for a specific VLAN.	
<i>vlan_id</i>	VLAN identifier.	
<b>features</b>	Displays IPv6 next-hop registered features.	
<b>policies</b>	Displays IPv6 next-hop policies.	
<b>ra-throttle</b>	Displays RA throttle information.	
<b>statistics</b>	Displays RA throttle statistics.	
<b>routers</b>	Displays RA throttle routers.	
<b>summary</b>	Displays the IPv6 neighbor binding table.	
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines**

DHCPv6 counters are applicable only for IPv6 bridging mode.

The following is the output of the **show ipv6 neighbor-binding summary** command:

```
(Cisco Controller) >show ipv6 neighbor-binding summary
Binding Table has 6 entries, 5 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DDCP
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk          0004:Orig access
0008:Orig trusted access    0010:Orig trusted trunk  0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned
   IPv6 address                MAC Address            Port VLAN Type      prlvl age
   state      Time left
-----
ND fe80::216:46ff:fe43:eb01      00:16:46:43:eb:01      1  980 wired          0005
  2 REACHABLE 157
ND fe80::9cf9:b009:b1b4:1ed9    70:f1:a1:dd:cb:d4      AP 980 wireless      0005
  2 REACHABLE 157
ND fe80::6233:4bff:fe05:25ef    60:33:4b:05:25:ef      AP 980 wireless      0005
  2 REACHABLE 203
ND fe80::250:56ff:fe8b:4a8f     00:50:56:8b:4a:8f      AP 980 wireless      0005
  2 REACHABLE 157
ND 2001:410:0:1:51be:2219:56c6:a8ad 70:f1:a1:dd:cb:d4      AP 980 wireless      0005
  5 REACHABLE 157
S 2001:410:0:1::9              00:00:00:00:00:08      AP 980 wireless      0100
  1 REACHABLE 205
```

The following is the output of the **show ipv6 neighbor-binding detailed** command:

```
(Cisco Controller) >show ipv6 neighbor-binding detailed mac 60:33:4b:05:25:ef
macDB has 3 entries for mac 60:33:4b:05:25:ef, 3 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DDCP
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk          0004:Orig access
0008:Orig trusted access    0010:Orig trusted trunk  0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned
   IPv6 address                MAC Address            Port VLAN Type      prlvl age
   state      Time left
-----
ND fe80::6233:4bff:fe05:25ef    60:33:4b:05:25:ef      AP 980 wireless      0009
  0 REACHABLE 303
ND 2001:420:0:1:6233:4bff:fe05:25ef 60:33:4b:05:25:ef      AP 980 wireless      0009
  0 REACHABLE 300
ND 2001:410:0:1:6233:4bff:fe05:25ef 60:33:4b:05:25:ef      AP 980 wireless      0009
  0 REACHABLE 301
```

The following is the output of the **show ipv6 neighbor-binding counters** command:

```
(Cisco Controller) >show ipv6 neighbor-binding counters
Received Messages

NDP Router Solicitation      6
NDP Router Advertisement    19
NDP Neighbor Solicitation    557
NDP Neighbor Advertisement  48
NDP Redirect                 0
NDP Certificate Solicit     0
NDP Certificate Advert       0
DHCPv6 Solicitation         0
```

```

DHCPv6 Advertisement          0
DHCPv6 Request                0
DHCPv6 Reply                  0
DHCPv6 Inform                 0
DHCPv6 Confirm                0
DHCPv6 Renew                  0
DHCPv6 Rebind                 0
DHCPv6 Release                0
DHCPv6 Decline                0
DHCPv6 Reconfigure            0
DHCPv6 Relay Forward          0
DHCPv6 Relay Rep              0

Bridged Messages

NDP Router Solicitation       6
NDP Router Advertisement     19
NDP Neighbor Solicitation    471
NDP Neighbor Advertisement   16
NDP Redirect                  0
NDP Certificate Solicit       0
NDP Certificate Advert        0
DHCPv6 Solicitation           0
DHCPv6 Advertisement         0
DHCPv6 Request                0
DHCPv6 Reply                  0
DHCPv6 Inform                 0
DHCPv6 Confirm                0
DHCPv6 Renew                  0
DHCPv6 Rebind                 0
DHCPv6 Release                0
DHCPv6 Decline                0
DHCPv6 Reconfigure            0
DHCPv6 Relay Forward          0
DHCPv6 Relay Rep              0
    
```

NDSUPPRESS Drop counters

```

total   silent ns_in_out ns_dad unicast multicast internal
-----
0       0       0       0       0       0       0
    
```

SNOOPING Drop counters

Dropped Msgs	total	silent	internal	CGA_vfy	RSA_vfy	limit	martian	martian_mac
no_trust not_auth stop								
NDP RS	0	0	0	0	0	0	0	0
NDP RA	0	0	0	0	0	0	0	0
NDP NS	0	0	0	0	0	0	0	0
NDP NA	0	0	0	0	0	0	0	0
NDP Redirect	0	0	0	0	0	0	0	0
NDP CERT SOL	0	0	0	0	0	0	0	0
NDP CERT ADV	0	0	0	0	0	0	0	0
DHCPv6 Sol	0	0	0	0	0	0	0	0
DHCPv6 Adv	0	0	0	0	0	0	0	0

## show ipv6 neighbor-binding

```

      0      0      0
DHCPv6 Req          0      0      0      0      0      0      0      0      0
      0      0      0
DHCPv6 Confirm     0      0      0      0      0      0      0      0      0
      0      0      0
DHCPv6 Renew       0      0      0      0      0      0      0      0      0
      0      0      0
DHCPv6 Rebind     0      0      0      0      0      0      0      0      0
      0      0      0
DHCPv6 Reply       0      0      0      0      0      0      0      0      0
      0      0      0
DHCPv6 Release     0      0      0      0      0      0      0      0      0
      0      0      0
DHCPv6 Decline    0      0      0      0      0      0      0      0      0
      0      0      0
DHCPv6 Recfg      0      0      0      0      0      0      0      0      0
      0      0      0
DHCPv6 Infreq     0      0      0      0      0      0      0      0      0
      0      0      0
DHCPv6 Relayfwd   0      0      0      0      0      0      0      0      0
      0      0      0
DHCPv6 Relayreply 0      0      0      0      0      0      0      0      0
      0      0      0

```

## CacheMiss Statistics

Multicast NS Forwarded

To STA 0

To DS 0

Multicast NS Dropped

To STA 467

To DS 467

## Multicast NA Statistics

Multicast NA Forwarded

To STA 0

To DS 0

Multicast NA Dropped

To STA 0

To DS 0

(Cisco Controller) &gt; &gt;

# show ipv6 ra-guard

To display the RA guard statistics, use the **show ipv6 ra-guard** command.

**show ipv6 ra-guard {ap | wlc} summary**

<b>Syntax Description</b>	<b>ap</b>	Displays Cisco access point details.
	<b>wlc</b>	Displays Cisco controller details.
	<b>summary</b>	Displays RA guard statistics.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example show the output of the **show ipv6 ra-guard ap summary** command:

```
(Cisco Controller) >show ipv6 ra-guard ap summary
IPv6 RA Guard on AP..... Enabled
RA Dropped per client:
MAC Address          AP Name              WLAN/GLAN      Number of RA Dropped
-----
00:40:96:b9:4b:89  Bhavik_1130_1_p13  2                19
-----
Total RA Dropped on AP..... 19
```

The following example shows how to display the RA guard statistics for a controller:

```
(Cisco Controller) >show ipv6 ra-guard wlc summary
IPv6 RA Guard on WLC..... Enabled
```

# show macfilter

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

```
show macfilter {summary | detailMAC | mesh | {wlan wlan-id}}
```

Syntax Description	summary	Displays a summary of all MAC filter entries.
	detail <i>MAC</i>	Displays details of a MAC filter entry.
	mesh	Display a summary of all MESH AP MAC filter entries.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** The MAC delimiter (none, colon, or hyphen) for MAC addresses sent to RADIUS servers is displayed. The MAC filter table lists the clients that are always allowed to associate with a wireless LAN.

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

```
(Cisco Controller) >show macfilter detail xx:xx:xx:xx:xx:xx
MAC Address..... xx:xx:xx:xx:xx:xx
WLAN Identifier..... Any
Interface Name..... management
Description..... RAP
```

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

```
(Cisco Controller) > show macfilter summary
MAC Filter RADIUS Compatibility mode..... Cisco ACS
MAC Filter Delimiter..... None
Local Mac Filter Table
MAC Address          WLAN Id          Description
-----
xx:xx:xx:xx:xx:xx   Any              RAP
xx:xx:xx:xx:xx:xx   Any              PAP2 (2nd hop)
xx:xx:xx:xx:xx:xx   Any              PAP1 (1st hop)
```



# show pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show pmk-cache** command.

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

<b>Syntax Description</b>	<b>all</b>	Displays information about all entries in the PMK cache.
	<i>MAC</i>	Information about a single entry in the PMK cache.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display information about a single entry in the PMK cache:

```
(Cisco Controller) >show pmk-cache xx:xx:xx:xx:xx:xx
```

The following example shows how to display information about all entries in the PMK cache:

```
(Cisco Controller) >show pmk-cache all
PMK Cache
Station              Entry
                    Lifetime  VLAN Override  IP Override
-----
-----
```

# show remote-lan

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

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

Syntax Description	summary	Displays a summary of all remote LANs.
	<i>remote-lan-id</i>	Remote LAN identifier.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

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

```
(Cisco Controller) >show remote-lan summary
Number of Remote LANS..... 2
RLAN ID  RLAN Profile Name                Status   Interface Name
-----  -
2         remote                                Disabled management
8         test                                  Disabled management
```

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

```
(Cisco Controller) >show remote-lan 2
Remote LAN Identifier..... 2
Profile Name..... remote
Status..... Disabled
MAC Filtering..... Disabled
AAA Policy Override..... Disabled
Network Admission Control
  Radius-NAC State..... Disabled
  SNMP-NAC State..... Disabled
  Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Number of Active Clients..... 0
Exclusionlist..... Disabled
Session Timeout..... Infinity
CHD per Remote LAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... management
Remote LAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Static IP client tunneling..... Disabled
Radius Servers
  Authentication..... Global Servers
  Accounting..... Global Servers
  Dynamic Interface..... Disabled
Security
  Web Based Authentication..... Enabled
```

```
ACL..... Unconfigured
Web Authentication server precedence:
1..... local
2..... radius
3..... ldap
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Disabled
```

# show rf-profile summary

To display a summary of RF profiles in the controller, use the **show rf-profile summary** command.

## show rf-profile summary

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

## Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is the output of the **show rf-profile summary** command:

```
(Cisco Controller) >show rf-profile summary
Number of RF Profiles..... 2
Out Of Box State..... Disabled
RF Profile Name          Band      Description          Applied
-----
T1a                      5 GHz    <none>              No
T1b                      2.4 GHz  <none>              No
```

# show rf-profile details

To display the RF profile details in the Cisco wireless LAN controller, use the **show rf-profile details** command.

**show rf-profile details** *rf-profile-name*

<b>Syntax Description</b>	<i>rf-profile-name</i>	Name of the RF profile.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following is the output of the **show rf-profile details** command:

```
(Cisco Controller) >show rf-profile details T1a
Description..... <none>
Radio policy..... 5 GHz
Transmit Power Threshold v1..... -70 dBm
Transmit Power Threshold v2..... -67 dBm
Min Transmit Power..... -10 dBm
Max Transmit Power..... 30 dBm

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
Max Clients..... 200
Client Trap Threshold..... 50
Multicast Data Rate..... 0
Rx Sop Threshold..... 0 dBm
Cca Threshold..... 0 dBm
Slot Admin State:..... Enabled
Band Select Probe Response..... Disabled
Band Select Cycle Count..... 2 cycles
Band Select Cycle Threshold..... 200 milliseconds
Band Select Expire Suppression..... 20 seconds
Band Select Expire Dual Band..... 60 seconds
Band Select Client Rssi..... -80 dBm
Load Balancing Denial..... 3 count
Load Balancing Window..... 5 clients
Coverage Data..... -80 dBm
Coverage Voice..... -80 dBm
Coverage Exception..... 3 clients
Coverage Level..... 25 %
```

## Related Topics

[show rf-profile summary](#), on page 284

[config rf-profile band-select](#), on page 60  
[config rf-profile client-trap-threshold](#), on page 62  
[config rf-profile create](#), on page 63  
[config rf-profile fra client-aware](#), on page 64  
[config rf-profile data-rates](#), on page 65  
[config rf-profile delete](#), on page 66  
[config rf-profile description](#), on page 67  
[config rf-profile load-balancing](#), on page 68  
[config rf-profile max-clients](#), on page 69  
[config rf-profile multicast data-rate](#), on page 70  
[config rf-profile out-of-box](#), on page 71  
[config rf-profile tx-power-control-thresh-v1](#), on page 72  
[config rf-profile tx-power-control-thresh-v2](#), on page 73  
[config rf-profile tx-power-max](#), on page 74  
[config rf-profile tx-power-min](#), on page 75

# show wlan

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

**show wlan** { **apgroups** | **summary** | *wlan\_id* | **foreignAp** | **lobby-admin-access** }

Syntax Description	apgroups	Displays access point group information.
	<b>summary</b>	Displays a summary of all wireless LANs.
	<i>wlan_id</i>	Displays the configuration of a WLAN. The Wireless LAN identifier range is from 1 to 512.
	<b>foreignAp</b>	Displays the configuration for support of foreign access points.
Command Default	None	
Usage Guidelines	For 802.1X client security type, which creates the PMK cache, the maximum session timeout that can be set is 86400 seconds when the session timeout is disabled. For other client security such as open, WebAuth, and PSK for which the PMK cache is not created, the session timeout value is shown as infinite when session timeout is disabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of wireless LANs for *wlan\_id* 1:

```
(Cisco Controller) >show wlan 1
WLAN Identifier..... 1
Profile Name..... aicha
Network Name (SSID)..... aicha
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Admission Control
  RADIUS Profiling Status ..... Disabled
  DHCP ..... Disabled
  HTTP ..... Disabled
Client Profiling Status ..... Disabled
  DHCP ..... Disabled
  HTTP ..... Disabled
  Radius-NAC State..... Enabled
  SNMP-NAC State..... Enabled
Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Maximum number of Clients per AP Radio..... 200
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
User Idle Timeout..... 300 seconds
```

```

User Idle Threshold..... 0 Bytes
NAS-identifier..... Talwar1
CHD per WLAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... management
Multicast Interface..... Not Configured
WLAN IPv4 ACL..... unconfigured
WLAN IPv6 ACL..... unconfigured
mDNS Status..... Disabled
mDNS Profile Name..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Static IP client tunneling..... Enabled
PMIPv6 Mobility Type..... none
Quality of Service..... Silver (best effort)
Per-SSID Rate Limits..... Upstream      Downstream
Average Data Rate..... 0              0
Average Realtime Data Rate..... 0        0
Burst Data Rate..... 0              0
Burst Realtime Data Rate..... 0        0
Per-Client Rate Limits..... Upstream      Downstream
Average Data Rate..... 0              0
Average Realtime Data Rate..... 0        0
Burst Data Rate..... 0              0
Burst Realtime Data Rate..... 0        0
Scan Defer Priority..... 4,5,6
Scan Defer Time..... 100 milliseconds
WMM..... Allowed
WMM UAPSD Compliant Client Support..... Disabled
Media Stream Multicast-direct..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
Passive Client Feature..... Disabled
IPv6 Support..... Disabled
Peer-to-Peer Blocking Action..... Disabled
Radio Policy..... All
DTIM period for 802.11a radio..... 1
DTIM period for 802.11b radio..... 1
Radius Servers
  Authentication..... Global Servers
  Accounting..... Global Servers
  Interim Update..... Disabled
  Dynamic Interface..... Disabled
Local EAP Authentication..... Enabled (Profile 'Controller_Local_EAP')

Security
  802.11 Authentication:..... Open System
  FT Support..... Disabled
  Static WEP Keys..... Disabled
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Enabled
      TKIP Cipher..... Disabled
      AES Cipher..... Enabled
    WPA2 (RSN IE)..... Enabled
      TKIP Cipher..... Disabled
      AES Cipher..... Enabled
Auth Key Management
  802.1x..... Enabled
  PSK..... Disabled
  CCKM..... Enabled

```



```

      FT(802.11r)..... Disabled
      FT-PSK(802.11r)..... Disabled
      PMF-1X(802.11w)..... Enabled
      PMF-PSK(802.11w)..... Disabled
FT Reassociation Timeout..... 20
FT Over-The-Air mode..... Enabled
FT Over-The-Ds mode..... Enabled
      GTK Randomization..... Disabled
      SKC Cache Support..... Disabled
      CCKM TSF Tolerance..... 1000
      Wi-Fi Direct policy configured..... Disabled
      EAP-Passthrough..... Disabled
CKIP ..... Disabled
      IP Security..... Disabled
      IP Security Passthru..... Disabled
      Web Based Authentication..... Disabled
      Web-Passthrough..... Disabled
      Conditional Web Redirect..... Disabled
      Splash-Page Web Redirect..... Disabled
      Auto Anchor..... Disabled
      FlexConnect Local Switching..... Enabled
      flexconnect Central Dhcp Flag..... Disabled
      flexconnect nat-pat Flag..... Disabled
      flexconnect Dns Override Flag..... Disabled
      FlexConnect Vlan based Central Switching ..... Disabled
      FlexConnect Local Authentication..... Disabled
      FlexConnect Learn IP Address..... Enabled
      Client MFP..... Optional
      PMF..... Disabled
      PMF Association Comeback Time..... 1
      PMF SA Query RetryTimeout..... 200
      Tkip MIC Countermeasure Hold-down Timer..... 60
Call Snooping..... Disabled
Roamed Call Re-Anchor Policy..... Disabled
SIP CAC Fail Send-486-Busy Policy..... Enabled
SIP CAC Fail Send Dis-Association Policy..... Disabled
KTS based CAC Policy..... Disabled
Band Select..... Disabled
Load Balancing..... Disabled
      Mobility Anchor List
      WLAN ID      IP Address      Status
      -----
802.11u..... Enabled
      Network Access type..... Chargeable Public Network
      Internet service..... Enabled
      Network Authentication type..... Not Applicable
      HESSID..... 00:00:00:00:00:00
      IP Address Type Configuration
      IPv4 Address type..... Available
      IPv6 Address type..... Not Known

      Roaming Consortium List
      Index      OUI List      In Beacon
      -----
          1      313131      Yes
          2      DDBBCC      No
          3      DDDDDD      Yes
      Realm configuration summary
      Realm index..... 1
      Realm name..... jobin
      EAP index..... 1
      EAP method..... Unsupported
      Index      Inner Authentication      Authentication Method
      -----

```

```

1          Credential Type          SIM
2  Tunneled Eap Credential Type    SIM
3          Credential Type          SIM
4          Credential Type          USIM
5          Credential Type          Hardware Token
6          Credential Type          SoftToken
Domain name configuration summary
  Index  Domain name
  -----
1       rom3
2       ram
3       rom1
Hotspot 2.0..... Enabled

Operator name configuration summary
  Index  Language  Operator name
  -----
1       ros     Robin

Port config summary
Index  IP protocol  Port number  Status
-----
1      1         1           0      Closed
2      1         1           0      Closed
3      1         1           0      Closed
4      1         1           0      Closed
5      1         1           0      Closed
6      1         1           0      Closed
7      1         1           0      Closed
WAN Metrics Info
Link status..... Up
Symmetric Link..... No
Downlink speed..... 4 kbps
Uplink speed..... 4 kbps
MSAP Services..... Disabled
Local Policy
-----
Priority  Policy Name
-----
1        Teacher_access_policy

```

The following example shows how to display a summary of all WLANs:

```

(Cisco Controller) >show wlan summary
Number of WLANs..... 1

WLAN ID  WLAN Profile Name / SSID          Status  Interface Name  PMIPv6
Mobility
-----
1        apsso / apsso                 Disabled management  none

```

The following example shows how to display the configuration for support of foreign access points:

```

(Cisco Controller) >show wlan foreignap
Foreign AP support is not enabled.

```

The following example shows how to display the AP groups:

```
(Cisco Controller) >show wlan apgroups
Total Number of AP Groups..... 1
Site Name..... APuser
Site Description..... <none>
Venue Name..... Not configured
Venue Group Code.....Unspecified
Venue Type Code.....Unspecified
Language Code..... Not configured
AP Operating Class..... 83,84,112,113,115,116,117,118,123
RF Profile
-----
2.4 GHz band..... <none>
5 GHz band..... <none>
WLAN ID      Interface      Network Admission Control      Radio Policy
-----
14           int_4          Disabled                        All
AP Name      Slots  AP Model      Ethernet MAC      Location      Port
Country  Priority
-----
Ibiza        2      AIR-CAP2602I-A-K9      44:2b:03:9a:8a:73      default location      1
US          1
Larch        2      AIR-CAP3502E-A-K9      f8:66:f2:ab:23:95      default location      1
US          1
Zest         2      AIR-CAP3502I-A-K9      00:22:90:91:6d:b6      ren      1
US          1

Number of Clients..... 1

MAC Address      AP Name      Status      Device Type
-----
24:77:03:89:9b:f8      ap2          Associated      Android
```

## test pmk-cache delete

To delete an entry in the Pairwise Master Key (PMK) cache from all Cisco wireless LAN controllers in the mobility group, use the **test pmk-cache delete** command.

**test pmk-cache delete** [**all** | *mac\_address*] {**local** | **global**}

Syntax Description		
<b>all</b>	Deletes PMK cache entries from all Cisco wireless LAN controllers.	
<i>mac_address</i>	MAC address of the Cisco wireless LAN controller from which PMK cache entries have to be deleted.	
<b>local</b>	Deletes PMK cache entries only on this WLC (default)	
<b>global</b>	Deletes PMK cache entries, for clients currently connected to this WLC, across the mobility group	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete all entries in the PMK cache:

```
(Cisco Controller) >test pmk-cache delete all
```