



Config Commands: a to i

- [config aaa auth, on page 9](#)
- [config aaa auth mgmt, on page 10](#)
- [config acl apply, on page 11](#)
- [config acl counter, on page 12](#)
- [config acl create, on page 13](#)
- [config acl cpu, on page 14](#)
- [config acl delete, on page 15](#)
- [config acl layer2, on page 16](#)
- [config acl rule, on page 18](#)
- [config acl url-acl, on page 20](#)
- [config acl url-acl apply, on page 21](#)
- [config acl url-acl external-server-ip, on page 22](#)
- [config acl url-acl list-type, on page 23](#)
- [config acl url-domain, on page 24](#)
- [config advanced 802.11 7920VSIEConfig, on page 25](#)
- [config advanced 802.11 channel add, on page 26](#)
- [config advanced 802.11 channel cleanair-event, on page 27](#)
- [config advanced 802.11 channel dca anchor-time, on page 28](#)
- [config advanced 802.11 channel dca chan-width-11n, on page 29](#)
- [config advanced 802.11 channel dca interval, on page 30](#)
- [config advanced 802.11 channel dca min-metric, on page 31](#)
- [config advanced 802.11 channel dca sensitivity, on page 32](#)
- [config advanced 802.11 channel foreign, on page 34](#)
- [config advanced 802.11 channel load, on page 35](#)
- [config advanced 802.11 channel noise, on page 36](#)
- [config advanced 802.11 channel outdoor-ap-dca, on page 37](#)
- [config advanced 802.11 channel pda-prop, on page 38](#)
- [config advanced 802.11 channel update, on page 39](#)
- [config advanced 802.11 coverage, on page 40](#)
- [config advanced 802.11 coverage exception global, on page 41](#)
- [config advanced 802.11 coverage fail-rate, on page 42](#)
- [config advanced 802.11 coverage level global, on page 43](#)
- [config advanced 802.11 coverage packet-count, on page 44](#)

- [config advanced 802.11 coverage rssi-threshold](#), on page 45
- [config advanced 802.11 edca-parameters](#), on page 47
- [config advanced 802.11 factory](#), on page 49
- [config advanced 802.11 group-member](#), on page 50
- [config advanced 802.11 group-mode](#), on page 51
- [config advanced 802.11 logging channel](#), on page 52
- [config advanced 802.11 logging coverage](#), on page 53
- [config advanced 802.11 logging foreign](#), on page 54
- [config advanced 802.11 logging load](#), on page 55
- [config advanced 802.11 logging noise](#), on page 56
- [config advanced 802.11 logging performance](#), on page 57
- [config advanced 802.11 logging txpower](#), on page 58
- [config advanced 802.11 monitor channel-list](#), on page 59
- [config advanced 802.11 monitor load](#), on page 60
- [config advanced 802.11 monitor measurement](#), on page 61
- [config advanced 802.11 monitor mode](#), on page 62
- [config advanced 802.11 monitor ndp-type](#), on page 63
- [config advanced 802.11 monitor timeout-factor](#), on page 64
- [config advanced 802.11 optimized roaming](#), on page 65
- [config advanced 802.11 packet](#), on page 66
- [config advanced 802.11 profile clients](#), on page 68
- [config advanced 802.11 profile customize](#), on page 69
- [config advanced 802.11 profile foreign](#), on page 70
- [config advanced 802.11 profile noise](#), on page 71
- [config advanced 802.11 profile throughput](#), on page 72
- [config advanced 802.11 profile utilization](#), on page 73
- [config advanced 802.11 receiver](#), on page 74
- [config advanced 802.11 reporting measurement](#), on page 75
- [config advanced 802.11 tpc-version](#), on page 76
- [config advanced 802.11 tpcv1-thresh](#), on page 77
- [config advanced 802.11 tpcv2-intense](#), on page 78
- [config advanced 802.11 tpcv2-per-chan](#), on page 79
- [config advanced 802.11 tpcv2-thresh](#), on page 80
- [config advanced 802.11 txpower-update](#), on page 81
- [config advanced eap](#), on page 82
- [config advanced fra service-priority](#), on page 84
- [config advanced fra client-aware client-select](#), on page 85
- [config advanced fra client-aware client-reset](#), on page 86
- [config advanced hyperlocation](#), on page 87
- [config advanced hyperlocation apgroup](#), on page 88
- [config advanced hyperlocation ble-beacon](#), on page 89
- [config advanced hyperlocation ble-beacon beacon-id](#), on page 90
- [config advanced hotspot](#), on page 91
- [config advanced timers auth-timeout](#), on page 92
- [config advanced timers eap-timeout](#), on page 93
- [config advanced timers eap-identity-request-delay](#), on page 94

- [config advanced timers](#), on page 95
- [config advanced fastpath fastcache](#), on page 98
- [config advanced fastpath pkt-capture](#), on page 99
- [config advanced sip-preferred-call-no](#), on page 100
- [config advanced sip-snooping-ports](#), on page 101
- [config advanced backup-controller primary](#), on page 102
- [config advanced backup-controller secondary](#), on page 103
- [config advanced client-handoff](#), on page 104
- [config advanced dot11-padding](#), on page 105
- [config advanced assoc-limit](#), on page 106
- [config advanced max-1x-sessions](#), on page 107
- [config advanced rate](#), on page 108
- [config advanced probe filter](#), on page 109
- [config advanced probe limit](#), on page 110
- [config advanced timers](#), on page 111
- [config ap 802.1Xuser](#), on page 114
- [config ap 802.1Xuser delete](#), on page 115
- [config ap 802.1Xuser disable](#), on page 116
- [config advanced dot11-padding](#), on page 117
- [config ap](#), on page 118
- [config ap aid-audit](#), on page 119
- [config ap antenna band-mode](#), on page 120
- [config ap atf 802.11](#), on page 121
- [config ap atf 802.11 client-access airtime-allocation](#), on page 122
- [config ap atf 802.11 policy](#), on page 123
- [config ap autoconvert](#), on page 124
- [config ap bhrate](#), on page 125
- [config ap bridgegroupname](#), on page 126
- [config ap bridging](#), on page 127
- [config ap cdp](#), on page 128
- [config ap cert-expiry-ignore](#), on page 130
- [config ap core-dump](#), on page 131
- [config ap crash-file clear-all](#), on page 132
- [config ap crash-file delete](#), on page 133
- [config ap crash-file get-crash-file](#), on page 134
- [config ap crash-file get-radio-core-dump](#), on page 135
- [config ap dhcp release-override](#), on page 136
- [config ap dtls-cipher-suite](#), on page 137
- [config ap dtls-version](#), on page 138
- [config ap ethernet duplex](#), on page 139
- [config ap ethernet tag](#), on page 140
- [config ap autoconvert](#), on page 141
- [config ap flexconnect central-dhcp](#), on page 142
- [config ap flexconnect local-split](#), on page 143
- [config ap flexconnect module-vlan](#), on page 144
- [config ap flexconnect policy](#), on page 145

- [config ap flexconnect radius auth set](#), on page 146
- [config ap flexconnect vlan](#), on page 147
- [config ap flexconnect vlan add](#), on page 148
- [config ap flexconnect vlan native](#), on page 149
- [config ap flexconnect vlan wlan](#), on page 150
- [config ap flexconnect web-auth](#), on page 151
- [config ap flexconnect web-policy acl](#), on page 152
- [config ap flexconnect wlan](#), on page 153
- [config ap group-name](#), on page 154
- [config ap hotspot](#), on page 155
- [config ap image predownload](#), on page 162
- [config ap image swap](#), on page 163
- [config ap ipsla](#), on page 164
- [config ap led-state](#), on page 165
- [config ap link-encryption](#), on page 166
- [config ap link-latency](#), on page 167
- [config ap location](#), on page 168
- [config ap logging syslog level](#), on page 169
- [config ap logging syslog facility](#), on page 170
- [config ap max-count](#), on page 172
- [config ap mgmtuser add](#), on page 173
- [config ap mgmtuser delete](#), on page 174
- [config ap mode](#), on page 175
- [config ap module3g](#), on page 177
- [config ap monitor-mode](#), on page 178
- [config ap name](#), on page 179
- [config ap packet-dump](#), on page 180
- [config ap port](#), on page 183
- [config ap power injector](#), on page 184
- [config ap power pre-standard](#), on page 185
- [config ap preferred-mode](#), on page 186
- [config ap primary-base](#), on page 187
- [config ap priority](#), on page 188
- [config ap reporting-period](#), on page 189
- [config ap reset](#), on page 190
- [config ap retransmit interval](#), on page 191
- [config ap retransmit count](#), on page 192
- [config ap role](#), on page 193
- [config ap rst-button](#), on page 194
- [config ap secondary-base](#), on page 195
- [config ap sniff](#), on page 196
- [config ap ssh](#), on page 197
- [config ap static-ip](#), on page 198
- [config ap stats-timer](#), on page 200
- [config ap syslog host global](#), on page 201
- [config ap syslog host specific](#), on page 202

- [config ap tcp-mss-adjust](#), on page 203
- [config ap telnet](#), on page 204
- [config ap tertiary-base](#), on page 205
- [config ap tftp-downgrade](#), on page 206
- [config ap username](#), on page 207
- [config ap venue](#), on page 208
- [config ap wlan](#), on page 212
- [config atf 802.11](#), on page 213
- [config atf policy](#), on page 214
- [config auth-list add](#), on page 215
- [config auth-list ap-policy](#), on page 216
- [config auth-list delete](#), on page 217
- [config avc profile create](#), on page 218
- [config avc profile delete](#), on page 219
- [config avc profile rule](#), on page 220
- [config band-select cycle-count](#), on page 222
- [config band-select cycle-threshold](#), on page 223
- [config band-select expire](#), on page 224
- [config band-select client-rssi](#), on page 225
- [config boot](#), on page 226
- [config call-home contact email address](#), on page 227
- [config call-home events](#), on page 228
- [config call-home http-proxy ipaddr](#), on page 229
- [config call-home http-proxy ipaddr 0.0.0.0](#), on page 230
- [config call-home profile](#), on page 231
- [config call-home profile delete](#), on page 232
- [config call-home profile status](#), on page 233
- [config call-home reporting](#), on page 234
- [config call-home tac-profile](#), on page 235
- [config cdp](#), on page 236
- [config certificate](#), on page 237
- [config certificate lsc](#), on page 238
- [config certificate ssc](#), on page 240
- [config certificate use-device-certificate webadmin](#), on page 241
- [config client ccx clear-reports](#), on page 242
- [config client ccx clear-results](#), on page 243
- [config client ccx default-gw-ping](#), on page 244
- [config client ccx dhcp-test](#), on page 245
- [config client ccx dns-ping](#), on page 246
- [config client ccx dns-resolve](#), on page 247
- [config client ccx get-client-capability](#), on page 248
- [config client ccx get-manufacturer-info](#), on page 249
- [config client ccx get-operating-parameters](#), on page 250
- [config client ccx get-profiles](#), on page 251
- [config client ccx log-request](#), on page 252
- [config client ccx send-message](#), on page 254

- [config client ccx stats-request](#), on page 258
- [config client ccx test-abort](#), on page 259
- [config client ccx test-association](#), on page 260
- [config client ccx test-dot1x](#), on page 261
- [config client ccx test-profile](#), on page 262
- [config client deauthenticate](#), on page 263
- [config client location-calibration](#), on page 264
- [config client profiling delete](#), on page 265
- [config cloud-services cmx](#), on page 266
- [config cloud-services server url](#), on page 267
- [config cloud-services server id-token](#), on page 268
- [config coredump](#), on page 269
- [config coredump ftp](#), on page 270
- [config coredump username](#), on page 271
- [config country](#), on page 272
- [config cts](#), on page 273
- [config cts ap](#), on page 274
- [config cts inline-tag](#), on page 275
- [config cts ap override](#), on page 276
- [config cts device-id](#), on page 277
- [config cts refresh](#), on page 278
- [config cts sxp ap connection delete](#), on page 279
- [config cts sxp ap connection peer](#), on page 280
- [config cts sxp ap default password](#), on page 281
- [config cts sxp ap listener](#), on page 282
- [config cts sxp ap reconciliation period](#), on page 283
- [config cts sxp ap retry period](#), on page 284
- [config cts sxp ap speaker](#), on page 285
- [config cts sxp](#), on page 286
- [config cts sxp connection](#), on page 287
- [config cts sxp default password](#), on page 288
- [config cts sxp retry period](#), on page 289
- [config cts sxp version](#), on page 290
- [config cts sxp](#), on page 291
- [config custom-web ext-webauth-mode](#), on page 292
- [config custom-web ext-webauth-url](#), on page 293
- [config custom-web ext-webserver](#), on page 294
- [config custom-web logout-popup](#), on page 295
- [config custom-web qrscan-bypass-opt](#) , on page 296
- [config custom-web radiusauth](#) , on page 297
- [config custom-web redirectUrl](#), on page 298
- [config custom-web sleep-client](#), on page 299
- [config custom-web webauth-type](#), on page 300
- [config custom-web weblogo](#), on page 301
- [config custom-web webmessage](#), on page 302
- [config custom-web webtitle](#), on page 303

- [config database size, on page 304](#)
- [config dhcp, on page 305](#)
- [config dhcp opt-82 format, on page 307](#)
- [config dhcp opt-82 remote-id, on page 308](#)
- [config dhcp proxy, on page 309](#)
- [config dhcp timeout, on page 310](#)
- [config dx, on page 311](#)
- [config exclusionlist, on page 312](#)
- [config fabric, on page 313](#)
- [config fabric vnid create name, on page 314](#)
- [config fabric control-plane enterprise-fabric , on page 315](#)
- [config fabric control-plane guest-fabric , on page 316](#)
- [config flexconnect \[ipv6\] acl, on page 317](#)
- [config flexconnect \[ipv6\] acl rule, on page 318](#)
- [config flexconnect \[ipv6\] acl url-domain, on page 320](#)
- [config flexconnect arp-caching, on page 321](#)
- [config flexconnect avc profile, on page 322](#)
- [config flexconnect fallback-radio-shut, on page 323](#)
- [config flexconnect group, on page 324](#)
- [config flexconnect group vlan, on page 329](#)
- [config flexconnect group *group-name* dhcp overridden-interface, on page 330](#)
- [config flexconnect group web-auth, on page 331](#)
- [config flexconnect group web-policy, on page 332](#)
- [config flexconnect join min-latency, on page 333](#)
- [config flexconnect office-extend, on page 334](#)
- [config flow, on page 335](#)
- [config guest-lan, on page 336](#)
- [config guest-lan custom-web ext-webauth-url, on page 337](#)
- [config guest-lan custom-web global disable, on page 338](#)
- [config guest-lan custom-web login_page, on page 339](#)
- [config guest-lan custom-web webauth-type, on page 340](#)
- [config guest-lan ingress-interface, on page 341](#)
- [config guest-lan interface, on page 342](#)
- [config guest-lan mobility anchor, on page 343](#)
- [config guest-lan nac, on page 344](#)
- [config guest-lan security, on page 345](#)
- [config interface 3g-vlan, on page 346](#)
- [config interface acl, on page 347](#)
- [config interface address, on page 348](#)
- [config interface address redundancy-management, on page 350](#)
- [config interface ap-manager, on page 351](#)
- [config interface create, on page 352](#)
- [config interface delete, on page 353](#)
- [config interface dhcp management, on page 354](#)
- [config interface dhcp, on page 356](#)
- [config interface dhcp dynamic-interface, on page 357](#)

- [config interface dhcp management option-6-opendns](#) , on page 358
- [config interface address](#), on page 359
- [config interface group failure-detect](#), on page 361
- [config interface group mdns-profile](#), on page 362
- [config interface guest-lan](#), on page 363
- [config interface hostname](#), on page 364
- [config interface nasid](#), on page 365
- [config interface nat-address](#), on page 366
- [config interface port](#), on page 367
- [config interface quarantine vlan](#), on page 368
- [config interface url-acl](#), on page 369
- [config interface vlan](#), on page 370
- [config interface mdns-profile](#), on page 371
- [config icons delete](#), on page 373
- [config icons file-info](#), on page 374
- [config ipv6 disable](#), on page 375
- [config ipv6 enable](#), on page 376
- [config ipv6 acl](#), on page 377
- [config ipv6 capwap](#), on page 379
- [config ipv6 interface](#), on page 380
- [config ipv6 multicast](#), on page 382
- [config ipv6 neighbor-binding](#), on page 383
- [config ipv6 ns-mcast-fwd](#), on page 385
- [config ipv6 ra-guard](#), on page 386
- [config ipv6 route](#), on page 387

config aaa auth

To configure the AAA authentication search order for management users, use the **config aaa auth** command.

```
config aaa auth mgmt [aaa_server_type1 | aaa_server_type2]
```

Syntax Description	mgmt	Configures the AAA authentication search order for controller management users by specifying up to three AAA authentication server types. The order that the server types are entered specifies the AAA authentication search order.
	aaa_server_type	(Optional) AAA authentication server type (local , radius , or tacacs). The local setting specifies the local database, the radius setting specifies the RADIUS server, and the tacacs setting specifies the TACACS+ server.
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 enter two AAA server types as long as one of the server types is local . You cannot enter radius and tacacs together.	
	<p>The following example shows how to configure the AAA authentication search order for controller management users by the authentication server type local:</p> <pre>(Cisco Controller) > config aaa auth radius local</pre>	
Related Commands	show aaa auth	

config aaa auth mgmt

To configure the order of authentication when multiple databases are configured, use the **config aaa auth mgmt** command.

config aaa auth mgmt [**radius** | **tacacs**]

Syntax Description	radius	(Optional) Configures the order of authentication for RADIUS servers.
	tacacs	(Optional) Configures the order of authentication for TACACS 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 configure the order of authentication for the RADIUS server:

```
(Cisco Controller) > config aaa auth mgmt radius
```

The following example shows how to configure the order of authentication for the TACACS server:

```
(Cisco Controller) > config aaa auth mgmt tacacs
```

Related Commands	show aaa auth order
------------------	----------------------------

config acl apply

To apply an access control list (ACL) to the data path, use the **config acl apply** command.

config acl apply *rule_name*

Syntax Description	<i>rule_name</i>	ACL name that contains 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.

Example

The following example shows how to apply an ACL to the data path:

```
(Cisco Controller) > config acl apply acl01
```

config acl counter

To see if packets are hitting any of the access control lists (ACLs) configured on your controller, use the **config acl counter** command.

config acl counter {start | stop}

Syntax Description	start	Enables ACL counters on your controller.
	stop	Disables ACL counters on your controller.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch. The following example shows how to enable ACL counters on your controller: (Cisco Controller) > config acl counter start	
Related Commands	clear acl counters	
	show acl detailed	

config acl create

To create a new access control list (ACL), use the **config acl create** command.

config acl create *rule_name*

Syntax Description	<i>rule_name</i>	ACL name that contains 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.
Usage Guidelines	<p>For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.</p> <p>The following example shows how to create a new ACL:</p> <pre>(Cisco Controller) > config acl create acl01</pre>	
Related Commands	show acl	

config acl cpu

To create a new access control list (ACL) rule that restricts the traffic reaching the CPU, use the **config acl cpu** command.

config acl cpu *rule_name* { **wired** | **wireless** | **both** }

Syntax Description	<i>rule_name</i>	Specifies the ACL name.
	wired	Specifies an ACL on wired traffic.
	wireless	Specifies an ACL on wireless traffic.
	both	Specifies an ACL on both wired and wireless traffic.

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 allows you to control the type of packets reaching the CPU.

The following example shows how to create an ACL named acl101 on the CPU and apply it to wired traffic:

```
(Cisco Controller) > config acl cpu acl101 wired
```

Related Commands	show acl cpu
------------------	--------------

config acl delete

To delete an access control list (ACL), use the **config acl delete** command.

config acl delete *rule_name*

Syntax Description	<i>rule_name</i>	ACL name that contains 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.
Usage Guidelines	<p>For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.</p> <p>The following example shows how to delete an ACL named acl101 on the CPU:</p> <pre>(Cisco Controller) > config acl delete acl101</pre>	
Related Commands	show acl	

config acl layer2

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

```
config acl layer2 { apply acl_name | create acl_name | delete acl_name | rule { action acl_name
index { permit | deny } | add acl_name index | change index acl_name old_index new_index |
delete acl_name index | etherType acl_name index etherType etherTypeMask | swap index acl_name
index1 index2 } }
```

Syntax Description

apply	Applies a Layer 2 ACL to the data path.
<i>acl_name</i>	Layer 2 ACL name. The name can be up to 32 alphanumeric characters.
create	Creates a Layer 2 ACL.
delete	Deletes a Layer 2 ACL.
rule	Configures a Layer 2 ACL rule.
action	Configures the action for the Layer 2 ACL rule.
<i>index</i>	Index of the Layer 2 ACL rule.
permit	Permits rule action.
deny	Denies rule action.
add	Creates a Layer 2 ACL rule.
change index	Changes the index of the Layer 2 ACL rule.
<i>old_index</i>	Old index of the Layer 2 ACL rule.
<i>new_index</i>	New index of the Layer 2 ACL rule.
delete	Deletes a Layer 2 ACL rule.
etherType	Configures the EtherType of a Layer 2 ACL rule.
<i>etherType</i>	EtherType of a Layer 2 ACL rule. EtherType is used to indicate the protocol that is encapsulated in the payload of an Ethernet frame. The range is a hexadecimal value from 0x0 to 0xffff.
<i>etherTypeMask</i>	Netmask of the EtherType. The range is a hexadecimal value from 0x0 to 0xffff.
swap index	Swaps the index values of two rules.
<i>index1 index2</i>	Index values of two Layer 2 ACL rules.

Command Default

The controller does not have any Layer2 ACLs.

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

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 controller.

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:

```
(Cisco Controller) >config acl layer2 apply acl_12_1
```

config acl rule

To configure ACL rules, use the **config acl rule** command.

```
config acl rule {action rule_name rule_index {permit | deny} | add rule_name rule_index |
change index rule_name old_index new_index | delete rule_name rule_index | destination address
rule_name rule_index ip_address netmask | destination port range rule_name rule_index start_port
end_port | direction rule_name rule_index {in | out | any} | dscp rule_name rule_index dscp
| protocol rule_name rule_index protocol | source address rule_name rule_index ip_address netmask
| source port range rule_name rule_index start_port end_port | swap index rule_name index_1 index_2 }
```

Syntax Description

action	Configures whether to permit or deny access.
<i>rule_name</i>	ACL name that contains up to 32 alphanumeric characters.
<i>rule_index</i>	Rule index between 1 and 32.
permit	Permits the rule action.
deny	Denies the rule action.
add	Adds a new rule.
change	Changes a rule's index.
index	Specifies a rule index.
delete	Deletes a rule.
destination address	Configures a rule's destination IP address and netmask.
destination port range	Configure a rule's destination port range.
<i>ip_address</i>	IP address of the rule.
<i>netmask</i>	Netmask of the rule.
<i>start_port</i>	Start port number (between 0 and 65535).
<i>end_port</i>	End port number (between 0 and 65535).
direction	Configures a rule's direction to in, out, or any.
in	Configures a rule's direction to in.
out	Configures a rule's direction to out.
any	Configures a rule's direction to any.
dscp	Configures a rule's DSCP.

<i>dscp</i>	Number between 0 and 63, or any .
protocol	Configures a rule's DSCP.
<i>protocol</i>	Number between 0 and 255, or any .
source address	Configures a rule's source IP address and netmask.
source port range	Configures a rule's source port range.
swap	Swaps two rules' indices.

Command Default

None

Command History

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

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to configure an ACL to permit access:

```
(Cisco Controller) > config acl rule action lab1 4 permit
```

Related Commands

show acl

config acl url-acl

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

config acl url-acl [**apply** | **create** | **delete** | **disable** | **enable** | **rule**]

config acl url-acl**apply** *acl-name*

config acl url-acl **create** *acl-name*

config acl url-acl **delete** *acl-name*

config acl url-acl**disable**

config acl url-acl**enable**

config acl url-acl**rule** [**action** | **add** | **delete** | **url**]

config acl url-acl**rule** **action** *acl-name index* {**permit** | **deny**}

config acl url-acl**rule** **add** *acl-name index*

config acl url-acl**rule** **delete** *acl-name index*

config acl url-acl**rule** **url** *acl-name index url-name*

Syntax Description		
apply <i>acl-name</i>		Enter URL ACL name up to 32 alphanumeric characters.
create		Create a new URL ACL.
delete		Delete URL ACL.
disable		Disable URL ACL feature.
enable		Enable URL ACL feature.
rule (action) (<i>acl-name</i>) (<i>index</i>)		Configures a rule's action in the URL ACL to either permit or deny. The <i>acl-name</i> contains up to 32 alphanumeric characters and URL ACL index up to 32 alphanumeric characters.
{ permit deny }		Permit or deny the url rule.
add <i>acl-name index</i>		Adds a new rule and rule index.
delete <i>acl-name index</i>		Deletes a rule and rule index.
url <i>acl-name index url-name</i>		Configures a rule's url address. Enter a url address and url name.

Command Default None

Command History	Release	Modification
	8.3	This command was introduced.

This example shows how to create a new URL ACL:

```
(Cisco Controller) >config acl url-acl create test
```

config acl url-acl apply

To apply a URL ACL to a data path, use the **config acl url-acl apply** command.

config acl url-acl apply

Syntax Description	apply	Applies URL ACL to the data path.
Command Default	None	
Command History	Release	Modification
	8.3	This command was introduced.

This example shows how to apply a URL ACL to a data path:

```
(Cisco Controller) >config acl url-acl apply
```

config acl url-acl external-server-ip

To redirect the user to a page which will be served when the requested URL is blocked. To configure the external server IP address, use the **config acl url-acl external-server-ip** command.

config acl url-acl external-server-ip *ip-address*

Syntax Description	external-server-ip	Specifies the ACL name.
	<i>ip-address</i>	Enter IP address of the external server.
Command Default	None	
Command History	Release	Modification
	8.4	This command was introduced.

The following example shows how to configure the external server IP address to redirect and show a page when the URL is blocked:

```
(Cisco Controller) > config acl url-acl external-server-ip 192.0.2.1
```

config acl url-acl list-type

To permit or deny traffic for rules in an given acl, use the **config acl url-acl list-type** command.

config acl url-acl list-type *acl_name*{**blacklist** | **whitelist**}

Syntax Description	list-type	Configure list-type for an URL ACL
	blacklist	All the rules will have action as deny.
	whitelist	All the rules will have action as permit.
Command Default	None	
Command History	Release	Modification
	8.4	This command was introduced.

The following example shows how to permit traffic for an ACL:

```
(Cisco Controller) > config acl url-acl list-type testacl whitelist
```

config acl url-domain

To add or delete an URL domain for the access control list, use the **config acl url-domain** command.

config acl url-domain{add | delete} *domain_name* *acl_name*

Syntax Description	<i>domain_name</i>	URL domain name for the access control list
	<i>acl_name</i>	Name of the access control list.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced.

The following example shows how to add a new URL domain for the access control list:

```
(Cisco Controller) > config acl url-domain add cisco.com android
```

The following example shows how to delete an existing URL domain from the access control list:

```
(Cisco Controller) > config acl url-domain delete play.google.com android
```


config advanced 802.11 7920VSIEConfig

To configure the Cisco unified wireless IP phone 7920 VISE parameters, use the **config advanced 802.11 7920VSIEConfig** command.

config advanced 802.11 { a | b } 7920VSIEConfig { call-admission-limit *limit* | G711-CU-Quantum *quantum* }

Syntax Description		
a		Specifies the 802.11a network.
b		Specifies the 802.11b/g network.
call-admission-limit		Configures the call admission limit for the 7920s.
G711-CU-Quantum		Configures the value supplied by the infrastructure indicating the current number of channel utilization units that would be used by a single G.711-20ms call.
<i>limit</i>		Call admission limit (from 0 to 255). The default value is 105.
<i>quantum</i>		G711 quantum value. The default value is 15.

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

Command History	<table> <tr> <th>Release</th> <th>Modification</th> </tr> <tr> <td>7.6</td> <td>This command was introduced in a release earlier than Release 7.6.</td> </tr> </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.				

This example shows how to configure the call admission limit for 7920 VISE parameters:

```
(Cisco Controller) >config advanced 802.11 7920VSIEConfig call-admission-limit 4
```

config advanced 802.11 channel add

To add channel to the 802.11 networks auto RF channel list, use the **config advanced 802.11 channel add** command.

config advanced 802.11 { **a** | **b** } **channel add** *channel_number*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	add	Adds a channel to the 802.11 network auto RF channel list.
	<i>channel_number</i>	Channel number to add to the 802.11 network auto RF channel list.
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 channel to the 802.11a network auto RF channel list:

(Cisco Controller) >**config advanced 802.11 channel add 132**

config advanced 802.11 channel cleanair-event

To configure CleanAir event driven Radio Resource Management (RRM) parameters for all 802.11 Cisco lightweight access points, use the **config advanced 802.11 channel cleanair-event** command.

config advanced 802.11 { a | b } channel cleanair-event { enable | disable | sensitivity [low | medium | high] | custom threshold *threshold_value* }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables the CleanAir event-driven RRM parameters.
	disable	Disables the CleanAir event-driven RRM parameters.
	sensitivity	Sets the sensitivity for CleanAir event-driven RRM.
	low	(Optional) Specifies low sensitivity.
	medium	(Optional) Specifies medium sensitivity
	high	(Optional) Specifies high sensitivity
	custom	Specifies custom sensitivity.
	threshold	Specifies the EDRRM AQ threshold value.
	<i>threshold_value</i>	Number of custom threshold.
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 CleanAir event-driven RRM parameters:

```
(Cisco Controller) > config advanced 802.11 channel cleanair-event enable
```

The following example shows how to configure high sensitivity for CleanAir event-driven RRM:

```
(Cisco Controller) > config advanced 802.11 channel cleanair-event sensitivity high
```

config advanced 802.11 channel dca anchor-time

To specify the time of day when the Dynamic Channel Assignment (DCA) algorithm is to start, use the **config advanced 802.11 channel dca anchor-time** command.

config advanced 802.11 { a | b } channel dca anchor-time *value*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	<i>value</i>	Hour of the time between 0 and 23. These values represent the hour from 12:00 a.m. to 11:00 p.m.
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 time of delay when the DCA algorithm starts:

```
(Cisco Controller) > config advanced 802.11 channel dca anchor-time 17
```

Related Commands	config advanced 802.11 channel dca interval
	config advanced 802.11 channel dca sensitivity
	config advanced 802.11 channel

config advanced 802.11 channel dca chan-width-11n

To configure the Dynamic Channel Assignment (DCA) channel width for all 802.11n radios in the 5-GHz band, use the **config advanced 802.11 channel dca chan-width-11n** command.

config advanced 802.11 { a | b } channel dca chan-width-11n { 20 | 40 | 80 }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	20	Sets the channel width for 802.11n radios to 20 MHz.
	40	Sets the channel width for 802.11n radios to 40 MHz.
	80	Sets the channel width for 802.11ac radios to 80-MHz.

Command Default The default channel width is 20.

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

Usage Guidelines If you choose 40, be sure to set at least two adjacent channels in the **config advanced 802.11 channel {add | delete} channel_number** command (for example, a primary channel of 36 and an extension channel of 40). If you set only one channel, that channel is not used for the 40-MHz channel width.

To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20- or 40-MHz mode using the **config 802.11 chan_width** command. If you then change the static configuration to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

The following example shows how to add a channel to the 802.11a network auto channel list:

```
(Cisco Controller) >config advanced 802.11a channel dca chan-width-11n 40
```

The following example shows how to set the channel width for the 802.11ac radio as 80-MHz:

```
(Cisco Controller) >config advanced 802.11a channel dca chan-width-11n 80
```

config advanced 802.11 channel dca interval

To specify how often the Dynamic Channel Assignment (DCA) is allowed to run, use the **config advanced 802.11 channel dca interval** command.

config advanced 802.11 { a | b } channel dca interval *value*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	<i>value</i>	Valid values are 0, 1, 2, 3, 4, 6, 8, 12, or 24 hours. 0 is 10 minutes (600 seconds).
Command Default	The default DCA channel interval is 10 (10 minutes).	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>If your controller supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.</p> <p>The following example shows how often the DCA algorithm is allowed to run:</p> <pre>(Cisco Controller) > config advanced 802.11 channel dca interval 8</pre>	
Related Commands	config advanced 802.11 dca anchor-time config advanced 802.11 dca sensitivity show advanced 802.11 channel	

config advanced 802.11 channel dca min-metric

To configure the 5-GHz minimum RSSI energy metric for DCA, use the **config advanced 802.11 channel dca min-metric** command.

config advanced 802.11 { **a** | **b** } **channel dca** *RSSI_value*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	<i>RSSI_value</i>	Minimum received signal strength indicator (RSSI) that is required for the DCA to trigger a channel change. The range is from –100 to –60 dBm.
Command Default	The default minimum RSSI energy metric for DCA is –95 dBm.	
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 minimum 5-GHz RSSI energy metric for DCA:

```
(Cisco Controller) > config advanced 802.11a channel dca min-metric -80
```

In the above example, the RRM must detect an interference energy of at least -80 dBm in RSSI for the DCA to trigger a channel change.

Related Commands	config advanced 802.11 dca interval
	config advanced 802.11 dca anchor-time
	show advanced 802.11 channel

config advanced 802.11 channel dca sensitivity

To specify how sensitive the Dynamic Channel Assignment (DCA) algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels, use the **config advanced 802.11 channel dca sensitivity** command.

config advanced 802.11 {a | b} channel dca sensitivity {low | medium | high}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
low	Specifies the DCA algorithm is not particularly sensitive to environmental changes. See the “Usage Guidelines” section for more information.
medium	Specifies the DCA algorithm is moderately sensitive to environmental changes. See the “Usage Guidelines” section for more information.
high	Specifies the DCA algorithm is highly sensitive to environmental changes. See the “Usage Guidelines” section for more information.

Command Default

None

Command History

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

Usage Guidelines

The DCA sensitivity thresholds vary by radio band as shown in the table below.

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 1: DCA Sensitivity Thresholds

Sensitivity	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

The following example shows how to configure the value of DCA algorithm’s sensitivity to low:

```
(Cisco Controller) > config advanced 802.11 channel dca sensitivity low
```

Related Commands

config advanced 802.11 dca interval

config advanced 802.11 dca anchor-time

show advanced 802.11 channel

config advanced 802.11 channel foreign

To have Radio Resource Management (RRM) consider or ignore foreign 802.11a interference avoidance in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel foreign** command.

config advanced 802.11 {a | b} channel foreign {enable | disable}

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables the foreign access point 802.11a interference avoidance in the channel assignment.
	disable	Disables the foreign access point 802.11a interference avoidance in the channel assignment.
Command Default	The default value for the foreign access point 802.11a interference avoidance in the channel assignment 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 have RRM consider foreign 802.11a interference when making channel selection updates for all 802.11a Cisco lightweight access points:

```
(Cisco Controller) > config advanced 802.11a channel foreign enable
```

Related Commands

- show advanced 802.11a channel
- config advanced 802.11b channel foreign

config advanced 802.11 channel load

To have Radio Resource Management (RRM) consider or ignore the traffic load in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel load** command.

config advanced 802.11 { a | b } channel load { enable | disable }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables the Cisco lightweight access point 802.11a load avoidance in the channel assignment.
	disable	Disables the Cisco lightweight access point 802.11a load avoidance in the channel assignment.
Command Default	The default value for Cisco lightweight access point 802.11a load avoidance in the channel assignment 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 have RRM consider the traffic load when making channel selection updates for all 802.11a Cisco lightweight access points:

```
(Cisco Controller) > config advanced 802.11 channel load enable
```

Related Commands

- show advanced 802.11a channel
- config advanced 802.11b channel load

config advanced 802.11 channel noise

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

config advanced 802.11 { **a** | **b** } **channel noise** { **enable** | **disable** }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables non-802.11a noise avoidance in the channel assignment. or ignore.
	disable	Disables the non-802.11a noise avoidance in the channel assignment.

Command Default	The default value for non-802.11a noise avoidance in the channel assignment 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 have RRM consider non-802.11a noise when making channel selection updates for all 802.11a Cisco lightweight access points:

```
(Cisco Controller) > config advanced 802.11 channel noise enable
```

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

config advanced 802.11 channel outdoor-ap-dca

To enable or disable the controller to avoid checking the non-Dynamic Frequency Selection (DFS) channels, use the **config advanced 802.11 channel outdoor-ap-dca** command.

config advanced 802.11 {a | b} channel outdoor-ap-dca {enable | disable}

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables 802.11 network DCA list option for outdoor access point.
	disable	Disables 802.11 network DCA list option for outdoor access point.
Command Default	The default value for 802.11 network DCA list option for outdoor access point is disabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>The config advanced 802.11 {a b} channel outdoor-ap-dca {enable disable} command is applicable only for deployments having outdoor access points such as 1522 and 1524.</p> <p>The following example shows how to enable the 802.11a DCA list option for outdoor access point:</p> <pre>(Cisco Controller) > config advanced 802.11a channel outdoor-ap-dca enable</pre>	
Related Commands	<p>show advanced 802.11a channel</p> <p>config advanced 802.11b channel noise</p>	

config advanced 802.11 channel pda-prop

To enable or disable propagation of persistent devices, use the **config advanced 802.11 channel pda-prop** command.

config advanced 802.11 {a | b} channel pda-prop {enable | disable}

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables the 802.11 network DCA list option for the outdoor access point.
	disable	Disables the 802.11 network DCA list option for the outdoor access point.
Command Default	The default 802.11 network DCA list option for the outdoor access point 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 or disable propagation of persistent devices:

```
(Cisco Controller) > config advanced 802.11 channel pda-prop enable
```

config advanced 802.11 channel update

To have Radio Resource Management (RRM) initiate a channel selection update for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel update** command.

config advanced 802.11 { a | b } channel update

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
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 initiate a channel selection update for all 802.11a network access points:

```
(Cisco Controller) > config advanced 802.11a channel update
```

config advanced 802.11 coverage

To enable or disable coverage hole detection, use the **config advanced 802.11 coverage** command.

config advanced 802.11 { a | b } coverage { enable | disable }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables the coverage hole detection.
	disable	Disables the coverage hole detection.

Command Default The default coverage hole detection value is enabled.

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

Usage Guidelines

If you enable coverage hole detection, the controller automatically determines, based on data that is received from the access points, whether any access points have clients that are potentially located in areas with poor coverage.

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to enable coverage hole detection on an 802.11a network:

```
(Cisco Controller) > config advanced 802.11a coverage enable
```

Related Commands

- config advanced 802.11 coverage exception global**
- config advanced 802.11 coverage fail-rate**
- config advanced 802.11 coverage level global**
- config advanced 802.11 coverage packet-count**
- config advanced 802.11 coverage rssi-threshold**

config advanced 802.11 coverage exception global

To specify the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point, use the **config advanced 802.11 coverage exception global** command.

config advanced 802.11 { a | b } coverage exception global percent

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	<i>percent</i>	Percentage of clients. Valid values are from 0 to 100%.
Command Default	The default percentage value for clients on an access point is 25%.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>If both the number and percentage of failed packets exceed the values that you entered in the config advanced 802.11 coverage packet-count and config advanced 802.11 coverage fail-rate commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the config advanced 802.11 coverage level global and config advanced 802.11 coverage exception global commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.</p> <p>The following example shows how to specify the percentage of clients for all 802.11a access points that are experiencing a low signal level:</p> <pre>(Cisco Controller) > config advanced 802.11 coverage exception global 50</pre>	
Related Commands	<p>config advanced 802.11 coverage exception global</p> <p>config advanced 802.11 coverage fail-rate</p> <p>config advanced 802.11 coverage level global</p> <p>config advanced 802.11 coverage packet-count</p> <p>config advanced 802.11 coverage rssi-threshold</p> <p>config advanced 802.11 coverage</p>	

config advanced 802.11 coverage fail-rate

To specify the failure rate threshold for uplink data or voice packets, use the **config advanced 802.11 coverage fail-rate** command.

config advanced 802.11 { **a** | **b** } **coverage** { **data** | **voice** } **fail-rate** *percent*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	data	Specifies the threshold for data packets.
	voice	Specifies the threshold for voice packets.
	<i>percent</i>	Failure rate as a percentage. Valid values are from 1 to 100 percent.

Command Default The default failure rate threshold uplink coverage fail-rate value is 20%.

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

Usage Guidelines If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to configure the threshold count for minimum uplink failures for data packets:

```
(Cisco Controller) > config advanced 802.11 coverage fail-rate 80
```

Related Commands

- config advanced 802.11 coverage exception global**
- config advanced 802.11 coverage level global**
- config advanced 802.11 coverage packet-count**
- config advanced 802.11 coverage rssi-threshold**
- config advanced 802.11 coverage**

config advanced 802.11 coverage level global

To specify the minimum number of clients on an access point with an received signal strength indication (RSSI) value at or below the data or voice RSSI threshold, use the **config advanced 802.11 coverage level global** command.

config advanced 802.11 { **a** | **b** } **coverage level global** *clients*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	<i>clients</i>	Minimum number of clients. Valid values are from 1 to 75.
Command Default	The default minimum number of clients on an access point is 3.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to specify the minimum number of clients on all 802.11a access points with an RSSI value at or below the RSSI threshold:

```
(Cisco Controller) > config advanced 802.11 coverage level global 60
```

Related Commands

- config advanced 802.11 coverage exception global**
- config advanced 802.11 coverage fail-rate**
- config advanced 802.11 coverage packet-count**
- config advanced 802.11 coverage rssi-threshold**
- config advanced 802.11 coverage**

config advanced 802.11 coverage packet-count

To specify the minimum failure count threshold for uplink data or voice packets, use the **config advanced 802.11 coverage packet-count** command.

config advanced 802.11 { **a** | **b** } **coverage** { **data** | **voice** } **packet-count** *packets*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	data	Specifies the threshold for data packets.
	voice	Specifies the threshold for voice packets.
	<i>packets</i>	Minimum number of packets. Valid values are from 1 to 255 packets.
Command Default	The default failure count threshold for uplink data or voice packets is 10.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>If both the number and percentage of failed packets exceed the values that you entered in the config advanced 802.11 coverage packet-count and config advanced 802.11 coverage fail-rate commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the config advanced 802.11 coverage level global and config advanced 802.11 coverage exception global commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.</p> <p>The following example shows how to configure the failure count threshold for uplink data packets:</p> <pre>(Cisco Controller) > config advanced 802.11 coverage packet-count 100</pre>	
Related Commands	config advanced 802.11 coverage exception global	
	config advanced 802.11 coverage fail-rate	
	config advanced 802.11 coverage level global	
	config advanced 802.11 coverage rssi-threshold	
	config advanced 802.11 coverage	

config advanced 802.11 coverage rssi-threshold

To specify the minimum receive signal strength indication (RSSI) value for packets that are received by an access point, use the **config advanced 802.11 coverage rssi-threshold** command.

config advanced 802.11 { a | b } coverage { data | voice } rssi-threshold *rssi*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	data	Specifies the threshold for data packets.
	voice	Specifies the threshold for voice packets.
	<i>rssi</i>	Valid values are from –60 to –90 dBm.

Command Default	• The default RSSI value for data packets is –80 dBm.
	• The default RSSI value for voice packets is –75 dBm.

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

Usage Guidelines The *rssi* value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data or voice queue with an RSSI value that is below the value that you enter, a potential coverage hole has been detected.

The access point takes RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to configure the minimum receive signal strength indication threshold value for data packets that are received by an 802.11a access point:

```
(Cisco Controller) > config advanced 802.11a coverage rssi-threshold -60
```

Related Commands	config advanced 802.11 coverage exception global
	config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage

config advanced 802.11 edca-parameters

To enable a specific Enhanced Distributed Channel Access (EDCA) profile on a 802.11a network, use the **config advanced 802.11 edca-parameters** command.

```
config advanced 802.11 { a | b } edca-parameters { wmm-default | svp-voice | optimized-voice |
optimized-video-voice | custom-voice | fastlane | custom-set { QoS Profile Name } {
aifs AP-value (0-16 ) Client value (0-16) | ecwmax AP-Value (0-10) Client value (0-10) | ecwmin
AP-Value (0-10) Client value (0-10) | txop AP-Value (0-255) Client value (0-255) } }
```

Syntax	Description
a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
wmm-default	Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option if voice or video services are not deployed on your network.
svp-voice	Enables Spectralink voice-priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls.
optimized-voice	Enables EDCA voice-optimized profile parameters. Choose this option if voice services other than Spectralink are deployed on your network.
optimized-video-voice	Enables EDCA voice-optimized and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network. Note If you deploy video services, admission control must be disabled.
custom-voice	Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.
fastlane	Enables fastlane on compatible devices.

custom-set

Enables customization of EDCA parameters

- **aifs**—Configures the Arbitration Inter-Frame Space.

AP Value (0-16) Client value (0-16)

- **ecwmax**—Configures the maximum Contention Window.

AP Value(0-10) Client Value (0-10)

- **ecwmin**—Configures the minimum Contention Window.

AP Value(0-10) Client Value(0-10)

- **txop**—Configures the Arbitration Transmission Opportunity Limit.

AP Value(0-255) Client Value(0-255)

QoS Profile Name - Enter the QoS profile name:

- bronze
- silver
- gold
- platinum

Command DefaultThe default EDCA parameter is **wmm-default**.**Command History**

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.2.110.0	In this release, custom-set keyword was added to edca-parameters command.
8.3	This command was modified and the fastlane keyword was added.

Examples

The following example shows how to enable Spectralink voice-priority parameters:

```
(Cisco Controller) > config advanced 802.11 edca-parameters svp-voice
```

Related Commands

config advanced 802.11b edca-parameters	Enables a specific Enhanced Distributed Channel Access (EDCA) profile on the 802.11a network.
show 802.11a	Displays basic 802.11a network settings.

config advanced 802.11 factory

To reset 802.11a advanced settings back to the factory defaults, use the **config advanced 802.11 factory** command.

config advanced 802.11 { a | b } factory

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
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 return all the 802.11a advanced settings to their factory defaults:

```
(Cisco Controller) > config advanced 802.11a factory
```

Related Commands	show advanced 802.11a channel
-------------------------	--------------------------------------

config advanced 802.11 group-member

To configure members in 802.11 static RF group, use the **config advanced 802.11 group-member** command.

config advanced 802.11 {a | b} group-member {add | remove} controller controller-ip-address

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	add	Adds a controller to the static RF group.
	remove	Removes a controller from the static RF group.
	controller	Name of the controller to be added.
	controller-ip-address	IP address of the controller to be added.
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 controller in the 802.11a automatic RF group:

```
(Cisco Controller) > config advanced 802.11a group-member add cisco-controller 209.165.200.225
```

Related Commands

- show advanced 802.11a group
- config advanced 802.11 group-mode

config advanced 802.11 group-mode

To set the 802.11a automatic RF group selection mode on or off, use the **config advanced 802.11 group-mode** command.

config advanced 802.11 { a | b } group-mode { auto | leader | off | restart }

Syntax Description		
a		Specifies the 802.11a network.
b		Specifies the 802.11b/g network.
auto		Sets the 802.11a RF group selection to automatic update mode.
leader		Sets the 802.11a RF group selection to static mode, and sets this controller as the group leader.
off		Sets the 802.11a RF group selection to off.
restart		Restarts the 802.11a RF group selection.

Command Default The default 802.11a automatic RF group selection mode is auto.

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 802.11a automatic RF group selection mode on:

```
(Cisco Controller) > config advanced 802.11a group-mode auto
```

The following example shows how to configure the 802.11a automatic RF group selection mode off:

```
(Cisco Controller) > config advanced 802.11a group-mode off
```

Related Commands

- show advanced 802.11a group
- config advanced 802.11 group-member

config advanced 802.11 logging channel

To turn the channel change logging mode on or off, use the **config advanced 802.11 logging channel** command.

config advanced 802.11 { a | b } logging channel { on | off }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	logging channel	Logs channel changes.
	on	Enables the 802.11 channel logging.
	off	Disables 802.11 channel logging.

Command Default	The default channel change logging mode is Off (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 turn the 802.11a logging channel selection mode on:

```
(Cisco Controller) > config advanced 802.11a logging channel on
```

Related Commands	show advanced 802.11a logging config advanced 802.11b logging channel
------------------	--

config advanced 802.11 logging coverage

To turn the coverage profile logging mode on or off, use the **config advanced 802.11 logging coverage** command.

config advanced 802.11 { a | b } logging coverage { on | off }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	on	Enables the 802.11 coverage profile violation logging.
	off	Disables the 802.11 coverage profile violation logging.

Command Default	The default coverage profile logging mode is Off (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 turn the 802.11a coverage profile violation logging selection mode on:

```
(Cisco Controller) > config advanced 802.11a logging coverage on
```

Related Commands	show advanced 802.11a logging config advanced 802.11b logging coverage
-------------------------	---

config advanced 802.11 logging foreign

To turn the foreign interference profile logging mode on or off, use the **config advanced 802.11 logging foreign** command.

config advanced 802.11 { a | b } logging foreign { on | off }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	on	Enables the 802.11 foreign interference profile violation logging.
	off	Disables the 802.11 foreign interference profile violation logging.
Command Default	The default foreign interference profile logging mode is Off (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 turn the 802.11a foreign interference profile violation logging selection mode on:

```
(Cisco Controller) > config advanced 802.11a logging foreign on
```

Related Commands

- show advanced 802.11a logging**
- config advanced 802.11b logging foreign**

config advanced 802.11 logging load

To turn the 802.11a load profile logging mode on or off, use the **config advanced 802.11 logging load** command.

config advanced 802.11 { a | b } logging load { on | off }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	on	Enables the 802.11 load profile violation logging.
	off	Disables the 802.11 load profile violation logging.
Command Default	The default 802.11a load profile logging mode is Off (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 turn the 802.11a load profile logging mode on:

```
(Cisco Controller) > config advanced 802.11 logging load on
```

Related Commands

- show advanced 802.11a logging
- config advanced 802.11b logging load

config advanced 802.11 logging noise

To turn the 802.11a noise profile logging mode on or off, use the **config advanced 802.11 logging noise** command.

config advanced 802.11 {a | b} logging noise {on | off}

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	on	Enables the 802.11 noise profile violation logging.
	off	Disables the 802.11 noise profile violation logging.
Command Default	The default 802.11a noise profile logging mode is off (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 turn the 802.11a noise profile logging mode on:

```
(Cisco Controller) > config advanced 802.11a logging noise on
```

Related Commands	show advanced 802.11a logging
	config advanced 802.11b logging noise

config advanced 802.11 logging performance

To turn the 802.11a performance profile logging mode on or off, use the **config advanced 802.11 logging performance** command.

config advanced 802.11 { a | b } logging performance { on | off }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	on	Enables the 802.11 performance profile violation logging.
	off	Disables the 802.11 performance profile violation logging.

Command Default	The default 802.11a performance profile logging mode is off (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 turn the 802.11a performance profile logging mode on:

```
(Cisco Controller) > config advanced 802.11a logging performance on
```

Related Commands	show advanced 802.11a logging config advanced 802.11b logging performance
-------------------------	--

config advanced 802.11 logging txpower

To turn the 802.11a transmit power change logging mode on or off, use the **config advanced 802.11 logging txpower** command.

config advanced 802.11 {a | b} logging txpower {on | off}

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	on	Enables the 802.11 transmit power change logging.
	off	Disables the 802.11 transmit power change logging.

Command Default	The default 802.11a transmit power change logging mode is off (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 turn the 802.11a transmit power change mode on:

```
(Cisco Controller) > config advanced 802.11 logging txpower off
```

Related Commands	show advanced 802.11 logging config advanced 802.11b logging power
-------------------------	---

config advanced 802.11 monitor channel-list

To set the 802.11a noise, interference, and rogue monitoring channel list, use the **config advanced 802.11 monitor channel-list** command.

config advanced 802.11 { a | b } monitor channel-list { all | country | dca }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	all	Monitors all channels.
	country	Monitors the channels used in the configured country code.
	dca	Monitors the channels used by the automatic channel assignment.

Command Default	The default 802.11a noise, interference, and rogue monitoring channel list is country.
------------------------	--

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

The following example shows how to monitor the channels used in the configured country:

```
(Cisco Controller) > config advanced 802.11 monitor channel-list country
```

Related Commands	show advanced 802.11a monitor coverage
-------------------------	--

config advanced 802.11 monitor load

To set the load measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor load** command.

config advanced 802.11 { **a** | **b** } **monitor load** *seconds*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	<i>seconds</i>	Load measurement interval between 60 and 3600 seconds.
Command Default	The default load measurement interval is 60 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 set the load measurement interval to 60 seconds:

```
(Cisco Controller) > config advanced 802.11 monitor load 60
```

Related Commands

- show advanced 802.11a monitor**
- config advanced 802.11b monitor load**

config advanced 802.11 monitor measurement

To set the signal measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor measurement** command.

config advanced 802.11 { a | b } monitor measurement *seconds*

Syntax Description	<i>seconds</i>	Signal measurement interval that you need to enter. Valid range is between 60 and 3600 seconds.
Command Default	The default signal measurement interval is 180 seconds.	
Command History	Release	Modification
	8.2	This command was introduced.

The following example shows how to set the signal measurement interval to 300 seconds:

```
(Cisco Controller) > config advanced 802.11 monitor measurement 300
```

config advanced 802.11 monitor mode

To enable or disable 802.11a access point monitoring, use the **config advanced 802.11 monitor mode** command.

config advanced 802.11 {a | b} monitor mode {enable | disable}

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	enable	Enables the 802.11 access point monitoring.
	disable	Disables the 802.11 access point monitoring.
Command Default	The default 802.11a access point monitoring 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 enable the 802.11a access point monitoring:

```
(Cisco Controller) > config advanced 802.11a monitor mode enable
```

Related Commands

- show advanced 802.11a monitor
- config advanced 802.11b monitor mode

config advanced 802.11 monitor ndp-type

To configure the 802.11 access point radio resource management (RRM) Neighbor Discovery Protocol (NDP) type, use the **config advanced 802.11 monitor ndp-type** command:


```
config advanced 802.11 { a | b } monitor ndp-type { protected | transparent }
```

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	protected	Specifies the Tx RRM protected NDP.
	transparent	Specifies the Tx RRM transparent NDP.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>Before you configure the 802.11 access point RRM NDP type, ensure that you have disabled the network by entering the config 802.11 disable network command.</p> <p>The following example shows how to enable the 802.11a access point RRM NDP type as protected:</p> <pre>(Cisco Controller) > config advanced 802.11 monitor ndp-type protected</pre>	
Related Commands	<p>config advanced 802.11 monitor</p> <p>config advanced 802.11 monitor mode</p> <p>config advanced 802.11 disable</p>	

config advanced 802.11 monitor timeout-factor

To configure the 802.11 neighbor timeout factor, use the **config advanced 802.11 monitor timeout-factor** command:

config advanced 802.11 {a | b} **monitor timeout-factor** *factor-value-in-minutes*

Syntax Description	<i>factor-value-in-minutes</i>		Neighbor timeout factor value that you must enter. Valid range is between 5 minutes to 60 minutes. We recommend that you set the timeout factor to 60 minutes.
Command Default	None		
Command History	Release	Modification	
	8.1	This command was introduced	
Usage Guidelines	If you are using Release 8.1 or a later release, we recommend that you set the timeout factor to 60 minutes. If the access point radio does not receive a neighbor packet from an existing neighbor within 60 minutes, the controller deletes the neighbor from the neighbor list.		
Note	 The Neighbor Timeout Factor was hardcoded to 60 minutes in Release 7.6, but was changed to 5 minutes in Release 8.0.100.0.		

config advanced 802.11 optimized roaming

To configure the optimized roaming parameters for each 802.11 band, use the **config advanced 802.11 optimized roaming** command.

config advanced {802.11a | 802.11b} optimized-roaming {enable | disable | interval *seconds* | datarate *mbps*}

Syntax Description	802.11a	Configures optimized roaming parameters for 802.11a network.
	802.11b	Configures optimized roaming parameters for 802.11b network.
	enable	Enables optimized roaming.
	disable	Disables optimized roaming.
	interval	Configures the client coverage reporting interval for 802.11a/b networks.
	<i>seconds</i>	Client coverage reporting interval in seconds. The range is from 5 to 90 seconds.
	datarate	Configures the threshold data rate for 802.11a/b networks.
	<i>mbps</i>	Threshold data rate in Mbps for 802.11a/b networks. For 802.11a, the configurable data rates are 6, 9, 12, 18, 24, 36, 48, and 54. For 802.11b, the configurable data rates are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54. You can configure 0 to disable the data rate for disassociating clients.
Command Default	By default, optimized roaming is disabled. The default value for client coverage reporting interval is 90 seconds and threshold data rate is 0 (disabled state).	
Command History	Release	Modification
	8.0	This command was introduced.
Usage Guidelines	<p>You must disable the 802.11a/b network before you configure the optimized roaming reporting interval. If you configure a low value for the reporting interval, the network can get overloaded with coverage report messages.</p> <p>The following example shows how to enable optimized roaming for the 802.11a network:</p> <pre>(Cisco Controller) > config advanced 802.11a optimized roaming enable</pre> <p>The following example shows how to configure the data rate interval for the 802.11a network:</p> <pre>(Cisco Controller) > config advanced 802.11a optimized roaming datarate 9</pre>	

config advanced 802.11 packet

To configure the maximum packet retries, consecutive packet failure thresholds, and the default timeout value, use **config advanced 802.11 packet** command.

config advanced 802.11{a | b} < QoS Profile Name > { **max-client-count** <threshold value (0-1000)> | **max-packet-count** <threshold value (0-1000)> | **max-retry** <maximum retry count> | **timeout** <time(in milliseconds)> }

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
<i>QoS Profile Name</i>	<ul style="list-style-type: none"> • bronze • silver • gold • platinum
max-client-count	<p>Configures the consecutive packet failure threshold before disassociating a client.</p> <p><i>threshold value</i> - Enter the client count threshold value in the range 0 to 1000</p>
max-packet-count	<p>Configures the consecutive packet failure threshold before not retrying failure packet.</p> <p><i>threshold value</i> - Enter the packet failure threshold value in the range 0 to 1000</p>
max-retry	<p>Configures the packet retry time for failure packet.</p> <p><i>maximum retry count</i> - Enter the maximum number of retries allowed.</p>
timeout	<p>Configures the packet aging or discard timeout threshold.</p> <p><i>time</i> - Enter the maximum time before the packet times out.</p>

Command Default

The default values for parameters in **config advanced 802.11 packet** command are:

Keyword	Default Value
max-client-count	500
max-packet-count	100
max-retry	3

Keyword	Default Value
timeout	35 milliseconds

Command History

Release	Modification
8.2	packet command was introduced in this release.

(Cisco Controller) > **config advanced 802.11a packet platinum max-packet-count 200**

Related Commands

show 802.11a	Displays basic 802.11a network settings.
---------------------	--

config advanced 802.11 profile clients

To set the Cisco lightweight access point clients threshold between 1 and 75 clients, use the **config advanced 802.11 profile clients** command.

config advanced 802.11 { **a** | **b** } **profile clients** { **global** | *cisco_ap* } *clients*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	global	Configures all 802.11a Cisco lightweight access points.
	<i>cisco_ap</i>	Cisco lightweight access point name.
	<i>clients</i>	802.11a Cisco lightweight access point client threshold between 1 and 75 clients.

Command Default	The default Cisco lightweight access point clients threshold is 12 clients.
------------------------	---

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 all Cisco lightweight access point clients thresholds to 25 clients:

```
(Cisco Controller) >config advanced 802.11 profile clients global 25
Global client count profile set.
```

The following example shows how to set the AP1 clients threshold to 75 clients:

```
(Cisco Controller) >config advanced 802.11 profile clients AP1 75
Global client count profile set.
```

config advanced 802.11 profile customize

To turn customizing on or off for an 802.11a Cisco lightweight access point performance profile, use the **config advanced 802.11 profile customize** command.

```
config advanced 802.11 { a | b } profile customize cisco_ap { on | off }
```

Syntax Description	a	Specifies the 802.11a/n network.
	b	Specifies the 802.11b/g/n network.
	<i>cisco_ap</i>	Cisco lightweight access point.
	on	Customizes performance profiles for this Cisco lightweight access point.
	off	Uses global default performance profiles for this Cisco lightweight access point.

Command Default	The default state of performance profile customization is Off.
-----------------	--

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

The following example shows how to turn performance profile customization on for 802.11a Cisco lightweight access point AP1:

```
(Cisco Controller) >config advanced 802.11 profile customize AP1 on
```

config advanced 802.11 profile foreign

To set the foreign 802.11a transmitter interference threshold between 0 and 100 percent, use the **config advanced 802.11 profile foreign** command.

config advanced 802.11 { **a** | **b** } **profile foreign** { **global** | *cisco_ap* } *percent*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	global	Configures all 802.11a Cisco lightweight access points.
	<i>cisco_ap</i>	Cisco lightweight access point name.
	<i>percent</i>	802.11a foreign 802.11a interference threshold between 0 and 100 percent.
Command Default	The default foreign 802.11a transmitter interference threshold value is 10.	
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 foreign 802.11a transmitter interference threshold for all Cisco lightweight access points to 50 percent:

```
(Cisco Controller) >config advanced 802.11a profile foreign global 50
```

The following example shows how to set the foreign 802.11a transmitter interference threshold for AP1 to 0 percent:

```
(Cisco Controller) >config advanced 802.11 profile foreign AP1 0
```

config advanced 802.11 profile noise

To set the 802.11a foreign noise threshold between –127 and 0 dBm, use the **config advanced 802.11 profile noise** command.

config advanced 802.11 { **a** | **b** } **profile noise** { **global** | *cisco_ap* } *dBm*

Syntax Description	a	Specifies the 802.11a/n network.
	b	Specifies the 802.11b/g/n network.
	global	Configures all 802.11a Cisco lightweight access point specific profiles.
	<i>cisco_ap</i>	Cisco lightweight access point name.
	<i>dBm</i>	802.11a foreign noise threshold between –127 and 0 dBm.

Command Default	The default foreign noise threshold value is –70 dBm.
------------------------	---

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 802.11a foreign noise threshold for all Cisco lightweight access points to –127 dBm:

```
(Cisco Controller) >config advanced 802.11a profile noise global -127
```

The following example shows how to set the 802.11a foreign noise threshold for AP1 to 0 dBm:

```
(Cisco Controller) >config advanced 802.11a profile noise AP1 0
```

config advanced 802.11 profile throughput

To set the Cisco lightweight access point data-rate throughput threshold between 1000 and 10000000 bytes per second, use the **config advanced 802.11 profile throughput** command.

config advanced 802.11 { **a** | **b** } **profile throughput** { **global** | *cisco_ap* } *value*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access point specific profiles.
<i>cisco_ap</i>	Cisco lightweight access point name.
<i>value</i>	802.11a Cisco lightweight access point throughput threshold between 1000 and 10000000 bytes per second.

Command Default

The default Cisco lightweight access point data-rate throughput threshold value is 1,000,000 bytes per second.

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 all Cisco lightweight access point data-rate thresholds to 1000 bytes per second:

```
(Cisco Controller) >config advanced 802.11 profile throughput global 1000
```

The following example shows how to set the AP1 data-rate threshold to 10000000 bytes per second:

```
(Cisco Controller) >config advanced 802.11 profile throughput AP1 10000000
```


config advanced 802.11 profile utilization

To set the RF utilization threshold between 0 and 100 percent, use the **config advanced 802.11 profile utilization** command. The operating system generates a trap when this threshold is exceeded.

config advanced 802.11 { a | b } profile utilization { global | cisco_ap } percent

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	global	Configures a global Cisco lightweight access point specific profile.
	<i>cisco_ap</i>	Cisco lightweight access point name.
	<i>percent</i>	802.11a RF utilization threshold between 0 and 100 percent.

Command Default	The default RF utilization threshold value is 80 percent.
-----------------	---

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 RF utilization threshold for all Cisco lightweight access points to 0 percent:

```
(Cisco Controller) >config advanced 802.11 profile utilization global 0
```

The following example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
(Cisco Controller) >config advanced 802.11 profile utilization AP1 100
```

config advanced 802.11 receiver

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

config advanced 802.11 { **a** | **b** } **receiver** { **default** | **rxstart jumpThreshold** *value* }

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	receiver	Specifies the receiver configuration.
	default	Specifies the default advanced receiver configuration.
	rxstart jumpThreshold	Specifies the receiver start signal.
		Note We recommend that you do not use this option as it is for Cisco internal use only.
	<i>value</i>	Jump threshold configuration value between 0 and 127.
Command Default	None	
Usage Guidelines	<ul style="list-style-type: none"> • Before you change the 802.11 receiver configuration, you must disable the 802.11 network. • We recommend that you do not use the rxstart jumpThreshold <i>value</i> option as it is for Cisco internal use only. 	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to prevent changes to receiver parameters while the network is enabled:

```
(Cisco Controller) > config advanced 802.11 receiver default
```

config advanced 802.11 reporting measurement

To set the reporting measurement interval between 60 and 3600 seconds,, use the **config advanced 802.11 reporting measurement** command.

config advanced 802.11 { a | b } reporting measurement *seconds*

Syntax Description	<i>seconds</i>	Reporting measurement interval that you need to enter. Valid range is between 60 and 3600 seconds.
Command Default	The default reporting measurement interval is 180 seconds.	
Command History	Release	Modification
	8.2	This command was introduced.

The following example shows how to set the signal measurement interval to 300 seconds:

```
(Cisco Controller) > config advanced 802.11 reporting measurement 300
```

config advanced 802.11 tpc-version

To configure the Transmit Power Control (TPC) version for a radio, use the **config advanced 802.11 tpc-version** command.

config advanced 802.11 {a | b} tpc-version {1 | 2}

Syntax Description	1	Specifies the TPC version 1 that offers strong signal coverage and stability.
	2	Specifies TPC version 2 is for scenarios where voice calls are extensively used. The Tx power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there could be higher roaming delays and coverage hole incidents.
Command Default	The default TPC version for a radio is 1.	
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 TPC version as 1 for the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11a tpc-version 1
```

Related Commands **config advanced 802.11 tpcv1-thresh**

config advanced 802.11 tpcv1-thresh

To configure the threshold for Transmit Power Control (TPC) version 1 of a radio, use the **config advanced 802.11 tpcv1-thresh** command.

config advanced 802.11 { a | b } tpcv1-thresh *threshold*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g/n network.
	<i>threshold</i>	Threshold value between –50 dBm to –80 dBm.
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 threshold as –60 dBm for TPC version 1 of the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11 tpcv1-thresh -60
```

Related Commands	config advanced 802.11 tpc-thresh
	config advanced 802.11 tpcv2-thresh

config advanced 802.11 tpcv2-intense

To configure the computational intensity for Transmit Power Control (TPC) version 2 of a radio, use the **config advanced 802.11 tpcv2-intense** command.

config advanced 802.11 { **a** | **b** } **tpcv2-intense** *intensity*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g/n network.
	<i>intensity</i>	Computational intensity value between 1 to 100.
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 computational intensity as 50 for TPC version 2 of the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11 tpcv2-intense 50
```

Related Commands	config advanced 802.11 tpc-thresh
	config advanced 802.11 tpcv2-thresh
	config advanced 802.11 tpcv2-per-chan

config advanced 802.11 tpcv2-per-chan

To configure the Transmit Power Control Version 2 on a per-channel basis, use the **config advanced 802.11 tpcv2-per-chan** command.

config advanced 802.11 { a | b } tpcv2-per-chan { enable | disable }

Syntax Description	enable	Enables the configuration of TPC version 2 on a per-channel basis.
	disable	Disables the configuration of TPC version 2 on a per-channel basis.

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 TPC version 2 on a per-channel basis for the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11 tpcv2-per-chan enable
```

Related Commands	config advanced 802.11 tpc-thresh
	config advanced 802.11 tpcv2-thresh
	config advanced 802.11 tpcv2-intense

config advanced 802.11 tpcv2-thresh

To configure the threshold for Transmit Power Control (TPC) version 2 of a radio, use the **config advanced 802.11 tpcv2-thresh** command.

config advanced 802.11 { **a** | **b** } **tpcv2-thresh** *threshold*

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
	<i>threshold</i>	Threshold value between –50 dBm to –80 dBm.
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 threshold as –60 dBm for TPC version 2 of the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11a tpcv2-thresh -60
```

Related Commands	config advanced 802.11 tpc-thresh
	config advanced 802.11 tpcv1-thresh
	config advanced 802.11 tpcv2-per-chan

config advanced 802.11 txpower-update

To initiate updates of the 802.11a transmit power for every Cisco lightweight access point, use the **config advanced 802.11 txpower-update** command.

config advanced 802.11 { a | b } txpower-update

Syntax Description	a	Specifies the 802.11a network.
	b	Specifies the 802.11b/g network.
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 initiate updates of 802.11a transmit power for an 802.11a access point:

```
(Cisco Controller) > config advanced 802.11 txpower-update
```

Related Commands	config advance 802.11b txpower-update
-------------------------	--

config advanced eap

To configure advanced extensible authentication protocol (EAP) settings, use the **config advanced eap** command.

config advanced eap { **bcast-key-interval** *seconds* | **eapol-key-timeout** *timeout* | **eapol-key-retries** *retries* | **identity-request-timeout** *timeout* | **identity-request-retries** *retries* | **key-index** *index* | **max-login-ignore-identity-response** {**enable** | **disable**} **request-timeout** *timeout* | **request-retries** *retries* } | **rsn-capability-validation** {**enable** | **disable** }

Syntax Description

bcast-key-interval <i>seconds</i>	Specifies the EAP-broadcast key renew interval time in seconds. The range is from 120 to 86400 seconds.
eapol-key-timeout <i>timeout</i>	Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK. The default value is 1000 milliseconds.
eapol-key-retries <i>retries</i>	Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
identity-request- timeout <i>timeout</i>	Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client. The default value is 30 seconds.
identity-request- retries	Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
key-index <i>index</i>	Specifies the key index (0 or 3) used for dynamic wired equivalent privacy (WEP).
max-login-ignore- identity-response	When enabled, this command ignores the limit set for the number of devices that can be connected to the controller with the same username using 802.1x authentication. When disabled, this command limits the number of devices that can be connected to the controller with the same username. This option is not applicable for Web auth user. Use the command config netuser maxUserLogin to set the limit of maximum number of devices per same username

enable	Ignores the same username reaching the maximum EAP identity response.
disable	Checks the same username reaching the maximum EAP identity response.
request-timeout	For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client. The default value is 30 seconds.
request-retries	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client. The default value is 2.
rsn-capability-validation {enable disable}	Allows you to enable or disable RSN-capability (2-Byte in EAPOL-M2 frame) validation with respect to association request.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.5.151.0	The rsn-capability-validation parameter was added.
8.10	

The following example shows how to configure the key index used for dynamic wired equivalent privacy (WEP):

```
(Cisco Controller) > config advanced eap key-index 0
```

config advanced fra service-priority

To configure the Flexible Radio Assignment (FRA) service priority, use the **config advanced fra service-priority** command.

config advanced fra service-priority [**client-aware** | **coverage** | **service-assurance**]

Syntax Description	client-aware	Configure the FRA service priority to Client Aware.
	coverage	Configure the FRA service priority to Coverage.
	service-assurance	Configure the FRA service priority to Service Assurance. service-assurance is not supported in 8.5 release.
Command Default	None	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	8.5	This command was introduced.
Usage Guidelines	<p>The following example shows how to configure the FRA service priority to client-aware:</p> <pre>(Cisco Controller) > config advanced fra service-priority client-aware</pre> <p>The following example shows how to configure the FRA service priority to coverage:</p> <pre>(Cisco Controller) > config advanced fra service-priority coverage</pre>	
Related Commands	<p>config advanced fra client-aware client-select</p> <p>config advanced fra client-aware client-reset</p>	

config advanced fra client-aware client-select

To configure the utilization threshold for redundant dual-band radios to switch from Monitor mode to 5GHz client-serving role, use the **config advanced fra client-aware client-select** command.

config advanced fra client-aware client-select *percent*

Syntax Description	<i>percent</i>	Utilization percentage value ranges from 0 to 100.
		Note The client-select <i>percent</i> value must be greater than the client-reset <i>percent</i> value. If not, you get to see the following message: Input for Client Aware FRA Client Reset Utilization Threshold is out of range.
Command Default	The default percent value for client-select is 50%.	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	8.5	This command was introduced.
Usage Guidelines	The following example shows how to configure the utilization threshold for redundant dual-band radios to switch from Monitor mode to 5GHz client-serving role: (Cisco Controller) > config advanced fra client-aware client-select 20	
Related Commands	config advanced fra client-aware client-reset	

config advanced fra client-aware client-reset

To configure the utilization threshold for redundant dual-band radios to switch back from 5GHz client-serving role to Monitor mode, use the **config advanced fra client-aware client-reset** command.

config advanced fra client-aware client-reset *percent*

Syntax Description	<i>percent</i>	Utilization percentage value ranges from 0 to 100.
	Note	<p>If the client-reset <i>percent</i> value is greater than the client-select <i>percent</i> value, you get to see the following message:</p> <p>Input for Client Aware FRA Client Reset Utilization Threshold is out of range.</p>
Command Default	The default percent value for client-reset is 5%.	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	8.5	This command was introduced.
Usage Guidelines	<p>The following example shows how to configure the utilization threshold for redundant dual-band radios to switch back from 5GHz client-serving role to Monitor mode:</p> <pre>(Cisco Controller) > config advanced fra client-aware client-reset 15</pre>	
Related Commands	config advanced fra client-aware client-select	

config advanced hyperlocation

To configure Cisco Hyperlocation globally on all APs that have the Cisco Hyperlocation module, use the **config advanced hyperlocation** command.

config advanced hyperlocation {**enable** | **disable** | **ntp** *ipv4-addr* | **flag-unset** *ap-name* | **reset-threshold** *value* | **threshold** *value* | **trigger-threshold** *value*}

Syntax Description	enable	Enables Cisco Hyperlocation globally on all Cisco APs that have the Cisco Hyperlocation module.
	disable	Disables Cisco Hyperlocation globally on all Cisco APs that have the Cisco Hyperlocation module.
	ntp <i>ipv4-addr</i>	Sets up the NTP server for Cisco Hyperlocation. Enter the IPv4 address of the NTP server that all APs that are involved in this calculation need to synchronize to.
	flag-unset <i>ap-name</i>	Configures the AP specified to accept any other level of Cisco Hyperlocation configuration.
	reset-threshold <i>value</i>	Configures PRL reset threshold value below which RSSI is ignored while sending to controller.
	reset-threshold <i>value</i>	Configures the threshold value below which RSSI is ignored while sending to controller.
	trigger-threshold <i>value</i>	Configures the number of scan cycles between PAK RSSI location trigger.

Command Default Disabled

Usage Guidelines

- Cisco Hyperlocation in enabled state has an impact on performance where both radios of APs that do not have Cisco Hyperlocation module go off-channel for about 100 milliseconds every 3 seconds.
- We recommend that you use the same NTP server that is used by the general controller infrastructure. The scans from multiple AP need to be synchronized for the location to be accurately calculated.

Command History

Release	Modification
8.1	This command was introduced.

This example shows how to enable Cisco Hyperlocation on all APs:

```
(Cisco Controller) >config advanced hyperlocation enable
```

config advanced hyperlocation apgroup

To configure Cisco Hyperlocation for an AP group that contains APs with the Cisco Hyperlocation module, use the **config advanced hyperlocation apgroup** command.

config advanced hyperlocation apgroup *group-name* {**enable** | **disable**}

config advanced hyperlocation apgroup *group-name* **ntp** *server-ipv4-address*

Syntax Description	enable	Enables Cisco Hyperlocation for the AP group that contains APs with the Cisco Hyperlocation module
	disable	Disables Cisco Hyperlocation for the AP group that contains APs with the Cisco Hyperlocation module
	ntp	Configures NTP server for the AP group.
	<i>server-ipv4-address</i>	IPv4 address of the NTP server for the AP group.
Command Default	Disabled	
Usage Guidelines	Cisco Hyperlocation in enabled state has an impact on performance where both radios of APs that do not have Cisco Hyperlocation module go off-channel for about 100 milliseconds every 3 seconds.	
Command History	Release	Modification
	8.1	This command was introduced.

This example shows how to enable Cisco Hyperlocation for an AP group:

```
(Cisco Controller) >config advanced hyperlocation apgroup myapgroup enable
```


config advanced hyperlocation ble-beacon

To configure BLE beacon parameters, use the **config advanced hyperlocation ble-beacon** command.

config advanced hyperlocation ble-beacon {**advertised-power** *rss-value* | **interval** *value* | **ap-name** *ap-name* | {**advertised-power** *rss-value* | **interval** *value* | **unset**}}

Syntax Description	advertised-power <i>rss-value</i>	Configures BLE advertised transmit power for all APs. Valid range is between -40 dBm to -100 dBm
	interval <i>value</i>	Configures BLE beacon interval for all APs. Valid range is between 1 to 10 seconds.
	ap-name <i>ap-name</i>	Configures BLE beacon parameters for the specified AP.
	unset	Clears AP-specific BLE configuration and sets global BLE configuration when applied.

Command History	Release	Modification
	8.1	This command was introduced.

This example shows how to set the BLE beacon interval for all APs to 8 seconds:

```
(Cisco Controller) >config advanced hyperlocation ble-beacon interval 8
```

config advanced hyperlocation ble-beacon beacon-id

To configure BLE beacon parameters for a specific beacon, use the **config advanced hyperlocation ble-beacon beacon-id** command.

```
config advanced hyperlocation ble-beacon beacon-id id {{delete | enable | disable } | add {txpwr value
| uuid value} | add ap-group group-name {enable | disable | major mjr-value | minor mnr-value |
txpwr value | uuid value} | add ap-name ap-name {enable | disable | major mjr-value | minor mnr-value
| txpwr value | uuid value}}
```

Syntax Description		
beacon-id <i>id</i>		Configures BLE parameters for the beacon ID that you enter. Valid range is between 1 to 5.
delete		Deletes the BLE beacon.
enable		Enables the BLE beacon.
disable		Disables the BLE beacon.
add		Adds a BLE beacon.
txpwr <i>value</i>		Configures the BLE attenuation level. You can choose to configure this for all APs, an AP group, or a specific AP. Valid range is between -52 dBm to 0.
uuid <i>value</i>		Configures universally unique identifier (UUID) for the beacon. You can choose to configure this for all APs, an AP group, or a specific AP. Enter a value in the xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx format.
ap-group <i>group-name</i>		Configures BLE beacon parameters for the AP group specified.
ap-name <i>ap-name</i>		Configures BLE beacon parameters for the AP specified.
major <i>mjr-value</i>		Configures major value for the BLE beacon. You can choose to configure this for an AP group or a specific AP.
minor <i>mnr-value</i>		Configures minor value for the BLE beacon. You can choose to configure this for an AP group or a specific AP.

Command History

Release	Modification
8.1	This command was introduced.

This example shows how to enable the BLE beacon with ID value as 3:

```
(Cisco Controller) >config advanced hyperlocation ble-beacon beacon-id 3 enable
```

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	anqp-4way	Enables, disables, or, configures the Access Network Query Protocol (ANQP) four way fragment threshold.
	disable	Disables the ANQP four way message.
	enable	Enables the ANQP four way message.
	threshold	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.
	cmbk-delay	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.
	garp	Disables or enables the Gratuitous ARP (GARP) forwarding to wireless network.
	disable	Disables the Gratuitous ARP (GARP) forwarding to wireless network.
	enable	Enables the Gratuitous ARP (GARP) forwarding to wireless network.
	gas-limit	Limits the number of Generic Advertisement Service (GAS) request action frames sent to the switch by an access point in a given interval.
	disable	Disables the GAS request action frame limit on access points.
	enable	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 advanced timers auth-timeout

To configure the authentication timeout, use the **config advanced timers auth-timeout** command.

config advanced timers auth-timeout *seconds*

Syntax Description	<i>seconds</i>	Authentication response timeout value in seconds between 10 and 600.
Command Default	The default authentication timeout value is 10 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 configure the authentication timeout to 20 seconds:

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config advanced timers eap-timeout

To configure the Extensible Authentication Protocol (EAP) expiration timeout, use the **config advanced timers eap-timeout** command.

config advanced timers eap-timeout *seconds*

Syntax Description	<i>seconds</i>	EAP timeout value in seconds between 8 and 120.
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 EAP expiration timeout to 10 seconds:

```
(Cisco Controller) >config advanced timers eap-timeout 10
```

config advanced timers eap-identity-request-delay

To configure the advanced Extensible Authentication Protocol (EAP) identity request delay in seconds, use the **config advanced timers eap-identity-request-delay** command.

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

Syntax Description	<i>seconds</i>	Advanced EAP identity request delay in number of seconds between 0 and 10.
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 advanced EAP identity request delay to 8 seconds:

```
(Cisco Controller) >config advanced timers eap-identity-request-delay 8
```

config advanced timers

To configure an advanced system timer, use the **config advanced timers** command.

```
config advanced timers { ap-coverage-report seconds | ap-discovery-timeout discovery-timeout |
ap-fast-heartbeat { local | flexconnect | all } { enable | disable } fast_heartbeat_seconds
| ap-heartbeat-timeout heartbeat_seconds | ap-primary-discovery-timeout primary_discovery_timeout
| ap-primed-join-timeout primed_join_timeout | auth-timeout auth_timeout | pkt-fwd-watchdog
{ enable | disable } { watchdog_timer | default } | eap-identity-request-delay
eap_identity_request_delay | eap-timeout eap_timeout }
```

Syntax	Description
ap-coverage-report	Configures RRM coverage report interval for all APs.
<i>seconds</i>	Configures the ap coverage report interval in seconds. The range is between 60 and 90 seconds. Default is 90 seconds.
ap-discovery-timeout	Configures the Cisco lightweight access point discovery timeout value.
<i>discovery-timeout</i>	Cisco lightweight access point discovery timeout value, in seconds. The range is from 1 to 10.
ap-fast-heartbeat	Configures the fast heartbeat timer, which reduces the amount of time it takes to detect a controller failure in access points.
local	Configures the fast heartbeat interval for access points in local mode.
flexconnect	Configures the fast heartbeat interval for access points in FlexConnect mode.
all	Configures the fast heartbeat interval for all the access points.
enable	Enables the fast heartbeat interval.
disable	Disables the fast heartbeat interval.
<i>fast_heartbeat_seconds</i>	Small heartbeat interval, which reduces the amount of time it takes to detect a controller failure, in seconds. The range is from 1 to 10.
ap-heartbeat-timeout	Configures Cisco lightweight access point heartbeat timeout value.
<i>heartbeat_seconds</i>	Cisco the Cisco lightweight access point heartbeat timeout value, in seconds. The range is from 1 to 30. This value should be at least three times larger than the fast heartbeat timer.
ap-primary-discovery-timeout	Configures the access point primary discovery request timer.
<i>primary_discovery_timeout</i>	Access point primary discovery request time, in seconds. The range is from 30 to 3600.
ap-primed-join-timeout	Configures the access point primed discovery timeout value.
<i>primed_join_timeout</i>	Access point primed discovery timeout value, in seconds. The range is from 120 to 43200.

auth-timeout	Configures the authentication timeout.
<i>auth_timeout</i>	Authentication response timeout value, in seconds. The range is from 10 to 600.
pkt-fwd-watchdog	Configures the packet forwarding watchdog timer to protect from fastpath deadlock.
<i>watchdog_timer</i>	Packet forwarding watchdog timer, in seconds. The range is from 60 to 300.
default	Configures the watchdog timer to the default value of 240 seconds.
eap-identity-request-delay	Configures the advanced Extensible Authentication Protocol (EAP) identity request delay, in seconds.
<i>eap_identity_request_delay</i>	Advanced EAP identity request delay, in seconds. The range is from 0 to 10.
eap-timeout	Configures the EAP expiration timeout.
<i>eap_timeout</i>	EAP timeout value, in seconds. The range is from 8 to 120.

Command Default

- The default access point discovery timeout is 10 seconds.
- The default access point heartbeat timeout is 30 seconds.
- The default access point primary discovery request timer is 120 seconds.
- The default authentication timeout is 10 seconds.
- The default packet forwarding watchdog timer is 240 seconds.

Command History

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

Usage Guidelines

The Cisco lightweight access point discovery timeout indicates how often a controller attempts to discover unconnected Cisco lightweight access points.

The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keepalive signal to the Cisco Wireless Controller.

The following example shows how to configure an access point discovery timeout with a timeout value of 20:

```
(Cisco Controller) >config advanced timers ap-discovery-timeout 20
```

The following example shows how to enable the fast heartbeat interval for an access point in FlexConnect mode:

```
(Cisco Controller) >config advanced timers ap-fast-heartbeat flexconnect enable 8
```


The following example shows how to configure the authentication timeout to 20 seconds:

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config advanced fastpath fastcache

To configure the fastpath fast cache control, use the **config advanced fastpath fastcache** command.

config advanced fastpath fastcache {enable | disable}

Syntax Description	enable	Enables the fastpath fast cache control.
	disable	Disables the fastpath fast cache control.

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 fastpath fast cache control:

```
(Cisco Controller) > config advanced fastpath fastcache enable
```

Related Commands **config advanced fastpath pkt-capture**

config advanced fastpath pkt-capture

To configure the fastpath packet capture, use the **config advanced fastpath pkt-capture** command.

config advanced fastpath pkt-capture {enable | disable}

Syntax Description	enable	Enables the fastpath packet capture.
	disable	Disables the fastpath packet capture.

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 fastpath packet capture:

```
(Cisco Controller) > config advanced fastpath pkt-capture enable
```

Related Commands	config advanced fastpath fastcache
------------------	------------------------------------

config advanced sip-preferred-call-no

To configure voice prioritization, use the **config advanced sip-preferred-call-no** command.

config advanced sip-preferred-call-no *call_index* { *call_number* | **none** }

Syntax Description

<i>call_index</i>	Call index with valid values between 1 and 6.
<i>call_number</i>	Preferred call number that can contain up to 27 characters.
none	Deletes the preferred call set for the specified index.

Command Default

None

Usage Guidelines

Before you configure voice prioritization, you must complete the following prerequisites:

- Set the voice to the platinum QoS level by entering the **config wlan qos wlan-id platinum** command.
- Enable the admission control (ACM) to this radio by entering the **config 802.11 {a | b} cac {voice | video} acm enable** command.
- Enable the call-snooping feature for a particular WLAN by entering the **config wlan call-snoop enable wlan-id** command.

To view statistics about preferred calls, enter the **show ap stats {802.11 {a | b} | wlan} cisco_ap** command.

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 new preferred call for index 2:

```
(Cisco Controller) > config advanced sip-preferred-call-no 2 0123456789
```

Related Commands

config wlan qos
config 802.11 cac video acm
config 802.11 cac voice acm
config wlan call-snoop
show ap stats

config advanced sip-snooping-ports

To configure call snooping ports, use the **config advanced sip-snooping-ports** command.

config advanced sip-snooping-ports *start_port end_port*

Syntax Description

start_port Starting port for call snooping. The range is from 0 to 65535.

end_port Ending port for call snooping. The range is from 0 to 65535.

Usage Guidelines

If you need only a single port for call snooping, configure the start and end port with the same number. The port used by the CIUS tablet is 5060 and the port range used by Facetime is from 16384 to 16402.

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 call snooping ports:

```
(Cisco Controller) > config advanced sip-snooping-ports 4000 4500
```

Related Commands

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video sip

config 802.11 cac voice sip

show advanced sip-preferred-call-no

show advanced sip-snooping-ports

debug cac

config advanced backup-controller primary

To configure a primary backup controller, use the **config advanced backup-controller primary** command.

config advanced backup-controller primary *system name IP addr*

Syntax Description	<i>system name</i>	Configures primary secondary backup controller.
	<i>IP addr</i>	IP address of the backup controller.

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 both IPv4 and IPv6 address formats.

Usage Guidelines To delete a primary backup controller entry (IPv6 or IPv4), enter 0.0.0.0 for the controller IP address.

The following example shows how to configure the IPv4 primary backup controller:

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 10.10.10.10
```

The following example shows how to configure the IPv6 primary backup controller:

```
(Cisco Controller) >config advanced backup-controller primary systemname 2001:9:6:40::623
```

The following example shows how to remove the IPv4 primary backup controller:

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 10.10.10.10
```

The following example shows how to remove the IPv6 primary backup controller:

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 0.0.0.0
```

Related Commands **show advanced back-up controller**

config advanced backup-controller secondary

To configure a secondary backup controller, use the **config advanced backup-controller secondary** command.

config advanced backup-controller secondary *system name IP addr*

Syntax Description	<i>system name</i>	Configures primary secondary backup controller.
	<i>IP addr</i>	IP address of the backup controller.

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 both IPv4 and IPv6 address formats.

Usage Guidelines	To delete a secondary backup controller entry (IPv4 or IPv6), enter 0.0.0.0 for the controller IP address.
-------------------------	--

The following example shows how to configure an IPv4 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 10.10.10.10
```

The following example shows how to configure an IPv6 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 2001:9:6:40::623
```

The following example shows how to remove an IPv4 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 0.0.0.0
```

The following example shows how to remove an IPv6 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 0.0.0.0
```

Related Commands	show advanced back-up controller
-------------------------	---

config advanced client-handoff

To set the client handoff to occur after a selected number of 802.11 data packet excessive retries, use the **config advanced client-handoff** command.

config advanced client-handoff *num_of_retries*

Syntax Description

<i>num_of_retries</i>	Number of excessive retries before client handoff (from 0 to 255).
-----------------------	--

Command Default

The default value for the number of 802.11 data packet excessive retries is 0.

Command History

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

Usage Guidelines

This command is supported only for the 1000/1510 series access points.

This example shows how to set the client handoff to 100 excessive retries:

```
(Cisco Controller) >config advanced client-handoff 100
```


config advanced dot11-padding

To enable or disable over-the-air frame padding, use the **config advanced dot11-padding** command.

config advanced dot11-padding {enable | disable}

Syntax Description	enable	Enables the over-the-air frame padding.
	disable	Disables the over-the-air frame padding.
Command Default	The default over-the-air frame padding 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 over-the-air frame padding:

```
(Cisco Controller) > config advanced dot11-padding enable
```

Related Commands	debug dot11
	debug dot11 mgmt interface
	debug dot11 mgmt msg
	debug dot11 mgmt ssid
	debug dot11 mgmt state-machine
	debug dot11 mgmt station
	show advanced dot11-padding

config advanced assoc-limit

To configure the rate at which access point radios send association and authentication requests to the controller, use the **config advanced assoc-limit** command.

config advanced assoc-limit { **enable** [*number of associations per interval* | *interval*] | **disable** }

Syntax Description

enable	Enables the configuration of the association requests per access point.
disable	Disables the configuration of the association requests per access point.
<i>number of associations per interval</i>	(Optional) Number of association request per access point slot in a given interval. The range is from 1 to 100.
<i>interval</i>	(Optional) Association request limit interval. The range is from 100 to 10000 milliseconds.

Command Default

The default state of the command is disabled state.

Command History

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

Usage Guidelines

When 200 or more wireless clients try to associate to a controller at the same time, the clients no longer become stuck in the DHCP_REQD state when you use the **config advanced assoc-limit** command to limit association requests from access points.

The following example shows how to configure the number of association requests per access point slot in a given interval of 20 with the association request limit interval of 250:

```
(Cisco Controller) >config advanced assoc-limit enable 20 250
```

config advanced max-1x-sessions

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

config advanced max-1x-sessions *no_of_sessions*

Syntax Description	<i>no_of_sessions</i>	Number of maximum 802.1x session initiation per AP at a time. The range is from 0 to 255, where 0 indicates unlimited.
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 maximum number of simultaneous 802.1X sessions:

```
(Cisco Controller) >config advanced max-1x-sessions 200
```

config advanced rate

To configure switch control path rate limiting, use the **config advanced rate** command.

config advanced rate { **enable** | **disable** }

Syntax Description	enable	Enables the switch control path rate limiting feature.
	disable	Disables the switch control path rate limiting feature.
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 switch control path rate limiting:

```
(Cisco Controller) >config advanced rate enable
```

config advanced probe filter

To configure the filtering of probe requests forwarded from an access point to the controller, use the **config advanced probe filter** command.

config advanced probe filter {**enable** | **disable**}

Syntax Description	enable	Enables the filtering of probe requests.
	disable	Disables the filtering of probe requests.
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 filtering of probe requests forwarded from an access point to the controller:

```
(Cisco Controller) >config advanced probe filter enable
```

config advanced probe limit

To limit the number of probes sent to the WLAN controller per access point per client in a given interval, use the **config advanced probe limit** command.

config advanced probe limit *num_probes interval*

Syntax Description	<i>num_probes</i>	Number of probe requests (from 1 to 100) forwarded to the controller per client per access point radio in a given interval.
	<i>interval</i>	Probe limit interval (from 100 to 10000 milliseconds).
Command Default	The default number of probe requests is 2. The default interval is 500 milliseconds.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to set the number of probes per access point per client to 5 and the probe interval to 800 milliseconds:

```
(Cisco Controller) >config advanced probe limit 5 800
```

config advanced timers

To configure an advanced system timer, use the **config advanced timers** command.

```
config advanced timers { ap-coverage-report seconds | ap-discovery-timeout discovery-timeout |
ap-fast-heartbeat { local | flexconnect | all } { enable | disable } fast_heartbeat_seconds
| ap-heartbeat-timeout heartbeat_seconds | ap-primary-discovery-timeout primary_discovery_timeout
| ap-primed-join-timeout primed_join_timeout | auth-timeout auth_timeout | pkt-fwd-watchdog
{ enable | disable } { watchdog_timer | default } | eap-identity-request-delay
eap_identity_request_delay | eap-timeout eap_timeout }
```

Syntax	Description
ap-coverage-report	Configures RRM coverage report interval for all APs.
<i>seconds</i>	Configures the ap coverage report interval in seconds. The range is between 60 and 90 seconds. Default is 90 seconds.
ap-discovery-timeout	Configures the Cisco lightweight access point discovery timeout value.
<i>discovery-timeout</i>	Cisco lightweight access point discovery timeout value, in seconds. The range is from 1 to 10.
ap-fast-heartbeat	Configures the fast heartbeat timer, which reduces the amount of time it takes to detect a controller failure in access points.
local	Configures the fast heartbeat interval for access points in local mode.
flexconnect	Configures the fast heartbeat interval for access points in FlexConnect mode.
all	Configures the fast heartbeat interval for all the access points.
enable	Enables the fast heartbeat interval.
disable	Disables the fast heartbeat interval.
<i>fast_heartbeat_seconds</i>	Small heartbeat interval, which reduces the amount of time it takes to detect a controller failure, in seconds. The range is from 1 to 10.
ap-heartbeat-timeout	Configures Cisco lightweight access point heartbeat timeout value.
<i>heartbeat_seconds</i>	Cisco the Cisco lightweight access point heartbeat timeout value, in seconds. The range is from 1 to 30. This value should be at least three times larger than the fast heartbeat timer.
ap-primary-discovery-timeout	Configures the access point primary discovery request timer.
<i>primary_discovery_timeout</i>	Access point primary discovery request time, in seconds. The range is from 30 to 3600.
ap-primed-join-timeout	Configures the access point primed discovery timeout value.
<i>primed_join_timeout</i>	Access point primed discovery timeout value, in seconds. The range is from 120 to 43200.

auth-timeout	Configures the authentication timeout.
<i>auth_timeout</i>	Authentication response timeout value, in seconds. The range is from 10 to 600.
pkt-fwd-watchdog	Configures the packet forwarding watchdog timer to protect from fastpath deadlock.
<i>watchdog_timer</i>	Packet forwarding watchdog timer, in seconds. The range is from 60 to 300.
default	Configures the watchdog timer to the default value of 240 seconds.
eap-identity-request-delay	Configures the advanced Extensible Authentication Protocol (EAP) identity request delay, in seconds.
<i>eap_identity_request_delay</i>	Advanced EAP identity request delay, in seconds. The range is from 0 to 10.
eap-timeout	Configures the EAP expiration timeout.
<i>eap_timeout</i>	EAP timeout value, in seconds. The range is from 8 to 120.

Command Default

- The default access point discovery timeout is 10 seconds.
- The default access point heartbeat timeout is 30 seconds.
- The default access point primary discovery request timer is 120 seconds.
- The default authentication timeout is 10 seconds.
- The default packet forwarding watchdog timer is 240 seconds.

Command History

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

Usage Guidelines

The Cisco lightweight access point discovery timeout indicates how often a controller attempts to discover unconnected Cisco lightweight access points.

The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keepalive signal to the Cisco Wireless Controller.

The following example shows how to configure an access point discovery timeout with a timeout value of 20:

```
(Cisco Controller) >config advanced timers ap-discovery-timeout 20
```

The following example shows how to enable the fast heartbeat interval for an access point in FlexConnect mode:

```
(Cisco Controller) >config advanced timers ap-fast-heartbeat flexconnect enable 8
```


The following example shows how to configure the authentication timeout to 20 seconds:

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config ap 802.1Xuser

To configure the global authentication username and password for all access points currently associated with the controller as well as any access points that associate with the controller in the future, use the **config ap 802.1Xuser** command.

```
config ap 802.1Xuser add username ap-username password ap-password {all | cisco_ap}
```

Syntax Description

add username	Specifies to add a username.
<i>ap-username</i>	Username on the Cisco AP.
password	Specifies to add a password.
<i>ap-password</i>	Password.
<i>cisco_ap</i>	Specific access point.
all	Specifies all 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

You must enter a strong *password*. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

You can set the values for a specific access point.

This example shows how to configure the global authentication username and password for all access points:

```
(Cisco Controller) >config ap 802.1Xuser add username cisco123 password cisco2020 all
```

config ap 802.1Xuser delete

To force a specific access point to use the controller’s global authentication settings, use the **config ap 802.1Xuser delete** command.

config ap 802.1Xuser delete *cisco_ap*

Syntax Description	<i>cisco_ap</i>	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 example shows how to delete access point AP01 to use the controller’s global authentication settings:

(Cisco Controller) >**config ap 802.1Xuser delete AP01**

config ap 802.1Xuser disable

To disable authentication for all access points or for a specific access point, use the **config ap 802.1Xuser disable** command.

config ap 802.1Xuser disable { **all** | *cisco_ap* }

Syntax Description	disable	Disables authentication.
	all	Specifies all access points.
	<i>cisco_ap</i>	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 You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

The following example shows how to disable the authentication for access point cisco_ap1:

(Cisco Controller) >**config ap 802.1Xuser disable**

config advanced dot11-padding

To enable or disable over-the-air frame padding, use the **config advanced dot11-padding** command.

config advanced dot11-padding {enable | disable}

Syntax Description	enable	Enables the over-the-air frame padding.
	disable	Disables the over-the-air frame padding.
Command Default	The default over-the-air frame padding 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 over-the-air frame padding:

```
(Cisco Controller) > config advanced dot11-padding enable
```

Related Commands	debug dot11
	debug dot11 mgmt interface
	debug dot11 mgmt msg
	debug dot11 mgmt ssid
	debug dot11 mgmt state-machine
	debug dot11 mgmt station
	show advanced dot11-padding

config ap

To configure a Cisco lightweight access point or to add or delete a third-party (foreign) access point, use the **config ap** command.

```
config ap {{enable | disable} cisco_ap | {add | delete} MAC port {enable | disable} IP_address}
```

Syntax Description	enable	Enables the Cisco lightweight access point.
	disable	Disables the Cisco lightweight access point.
	cisco_ap	Name of the Cisco lightweight access point.
	add	Adds foreign access points.
	delete	Deletes foreign access points.
	MAC	MAC address of a foreign access point.
	port	Port number through which the foreign access point can be reached.
	IP_address	IP address of the foreign access point.
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 both IPv4 and IPv6.

The following example shows how to disable lightweight access point AP1:

```
(Cisco Controller) >config ap disable AP1
```

The following example shows how to add a foreign access point with MAC address 12:12:12:12:12:12 and IP address 192.12.12.1 from port 2033:

```
(Cisco Controller) >config ap add 12:12:12:12:12:12 2033 enable 192.12.12.1
```

config ap aid-audit

To configure the Cisco lightweight access point AID audit mechanism, use the **config ap aid-audit** command.

```
config ap aid-audit {enable | disable}
```

Syntax Description	aid-audit	Configures AID audit mechanism.
	enable	Enables AID audit mechanism.
	disable	Disables AID audit mechanism.

Command Default	Disabled.
-----------------	-----------

Command History	Release	Modification
	8.6	This command was introduced.

The following example shows how to enable AP aid-audit:

```
(Cisco Controller) >config ap aid-audit enable
```

config ap antenna band-mode

To configure a Cisco AP antenna's band mode as either single or dual, use the **config ap antenna band-mode** command.

config ap antenna band-mode {**single** | **dual**} *cisco-ap*

Syntax Description	single	Configures single band antenna mode for a Cisco AP.
	dual	Configures dual band antenna mode for a Cisco AP.
	<i>cisco-ap</i>	Cisco AP name.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced.
	8.3 and later releases	The antenna-band-mode parameter was modified to antenna band-mode .

config ap atf 802.11

Configure Cisco Airtime Fairness at an AP level by using the **config ap atf 802.11** command.

config ap atf 802.11{a | b} {mode {disable | monitor | enforce-policy} ap-name} | {optimization {enable | disable}}

Syntax Description		
a		Specifies the 802.11a network settings
b		Specifies the 802.11b/g network settings
mode		Configures the granularity of Cisco ATF enforcement
disable		Disables Cisco ATF
monitor		Configures Cisco ATF in monitor mode
enforce-policy		Configures Cisco ATF in enforcement mode
<i>ap-name</i>		AP name that you must specify
optimization		Configures airtime optimization
enable		Enables airtime optimization
disable		Disables airtime optimization

Command History	Release	Modification
	8.1	This command was introduced

To enable airtime optimization on an 802.11a network for a Cisco AP, *my-ap*, enter the following command:

```
(Cisco Controller) >config ap atf 802.11a optimization enable my-ap
```

config ap atf 802.11 client-access airtime-allocation

To configure override of ATF airtime allocation on mesh AP, use the **config ap atf 802.11 client-access airtime-allocation override {enable | disable}** command.

config ap atf 802.11 {a | b} client-access airtime-allocation %of-airtime-allocation-bw-5-to-90 mesh-ap-name override {enable | disable}

Syntax Description		
a		Specifies the 802.11a network settings
b		Specifies the 802.11b/g network settings
<i>%of-airtime-allocation-bw-5-to-90</i>		Percentage of airtime allocation for client access. Valid range is between 5 and 90. This percentage of airtime allocation impacts both the client and the uplink backhaul percentage.
<i>mesh-ap-name</i>		Name of the mesh AP
override		Allows override of ATF airtime allocation on the mesh AP
enable		Enables airtime allocation override
disable		Disables airtime allocation override

Command History	Release	Modification
	8.4	This command was introduced

On an 802.11a network, to configure override of ATF airtime allocation on a mesh AP, *map1*, enter the following command:

```
(Cisco Controller) >config ap atf 802.11a client-access airtime-allocation
10 override map1 enable
```

config ap atf 802.11 policy

To configure AP-level override for Cisco ATF policy on a WLAN, enter this command:

```
confit ap atf 802.11 {a | b} policy wlan-id policy-name ap-name override {enable | disable}
```

Syntax Description	
a	Specifies the 802.11a network settings
b	Specifies the 802.11b network settings
policy	Specifies the Cisco ATF policy
<i>wlan-id</i>	WLAN ID or Remote LAN ID that you must specify
<i>policy-name</i>	Cisco ATF policy name that you must specify
<i>ap-name</i>	Name of the AP that you must specify
override	Configures ATF policy override for a WLAN in the AP group
enable	Enables ATF policy override for a WLAN in the AP group
disable	Disables ATF policy override for a WLAN in the AP group

Command History	Release	Modification
	8.1	This command was introduced

config ap autoconvert

To automatically convert all access points to FlexConnect mode or Monitor mode upon associating with the controller, use the **config ap autoconvert** command.

config ap autoconvert { **flexconnect** | **monitor** | **disable** }

Syntax Description	flexconnect	Configures all the access points automatically to FlexConnect mode.
	monitor	Configures all the access points automatically to monitor mode.
	disable	Disables the autoconvert option on the 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

When access points in local mode connect to a Cisco 7500 Series Wireless Controller, they do not serve clients. The access point details are available in the controller. To enable access points to serve clients or perform monitoring related tasks when connected to the Cisco 7500 Series Wireless Controller, the access points must be in FlexConnect mode or Monitor mode.

The command can also be used for conversion of AP modes in Cisco 5520, 8540, and 8510 Series Wireless Controller platforms.

The following example shows how to automatically convert all access points to the FlexConnect mode:

```
(Cisco Controller) >config ap autoconvert flexconnect
```

The following example shows how to disable the autoconvert option on the APs:

```
(Cisco Controller) >config ap autoconvert disable
```

config ap bhrate

To configure the Cisco bridge backhaul Tx rate, use the **config ap bhrate** command.

```
config ap bhrate {rate | auto} cisco_ap
```

Syntax Description	rate	Cisco bridge backhaul Tx rate in kbps. The valid values are 6000, 12000, 18000, 24000, 36000, 48000, and 54000.
	auto	Configures the auto data rate.
	cisco_ap	Name of a Cisco lightweight access point.
Command Default	The default status of the command is set to Auto.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	When the bridge data rate is set to auto , the mesh backhaul chooses the highest rate where the next higher rate cannot be used due to unsuitable conditions for that specific rate (and not because of conditions that affect all rates).	

The following example shows how to configure the Cisco bridge backhaul Tx rate to 54000 kbps:

```
(Cisco Controller) >config ap bhrate 54000 AP01
```

config ap bridgegroupname

To set or delete a bridge group name on a Cisco lightweight access point, use the **config ap bridgegroupname** command.

config ap bridgegroupname {set *groupname* | delete | {strict-matching {enable | disable} }} *cisco_ap*

Syntax Description	set	Sets a Cisco lightweight access point's bridge group name.
	<i>groupname</i>	Bridge group name.
	delete	Deletes a Cisco lightweight access point's bridge group name.
	<i>cisco_ap</i>	Name of a Cisco lightweight access point.
	strict-matching	Restricts the possible parent list, if the MAP has a non-default BGN, and the potential parent has a different BGN
	enable	Enables a Cisco lightweight access point's group name.
	disable	Disables a Cisco lightweight access point's group name.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	The strict-matching parameter was added.
Usage Guidelines	<p>Only access points with the same bridge group name can connect to each other. Changing the AP bridgegroupname may strand the bridge AP.</p> <p>The following example shows how to delete a bridge group name on Cisco access point's bridge group name AP02:</p> <pre>(Cisco Controller) >config ap bridgegroupname delete AP02 Changing the AP's bridgegroupname may strand the bridge AP. Please continue with caution. Changing the AP's bridgegroupname will also cause the AP to reboot. Are you sure you want to continue? (y/n)</pre>	

config ap bridging

To configure Ethernet-to-Ethernet bridging on a Cisco lightweight access point, use the **config ap bridging** command.

config ap bridging { **enable** | **disable** } *cisco_ap*

Syntax Description	enable	Enables the Ethernet-to-Ethernet bridging on a Cisco lightweight access point.
	disable	Disables Ethernet-to-Ethernet bridging.
	<i>cisco_ap</i>	Name of a Cisco lightweight 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 example shows how to enable bridging on an access point:

```
(Cisco Controller) >config ap bridging enable nyc04-44-1240
```

The following example shows hot to disable bridging on an access point:

```
(Cisco Controller) >config ap bridging disable nyc04-44-1240
```

config ap cdp

To configure the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **config ap cdp** command.

config ap cdp {**enable** | **disable** | **interface** {**ethernet** *interface_number* | **slot** *slot_id*}} {*cisco_ap* | **all**}

Syntax Description

enable	Enables CDP on an access point.
disable	Disables CDP on an access point.
interface	Configures CDP in a specific interface.
ethernet	Configures CDP for an ethernet interface.
<i>interface_number</i>	Ethernet interface number between 0 and 3.
slot	Configures CDP for a radio interface.
<i>slot_id</i>	Slot number between 0 and 3.
<i>cisco_ap</i>	Name of a Cisco lightweight access point.
all	Specifies all access points.



Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

Command Default

Enabled on radio interfaces of mesh APs and disabled on radio interfaces of non-mesh APs. Enabled on Ethernet interfaces of all APs.

Command History

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

Usage Guidelines

The **config ap cdp disable all** command disables CDP on all access points that are joined to the controller and all access points that join in the future. CDP remains disabled on both current and future access points even after the controller or access point reboots. To enable CDP, enter the **config ap cdp enable all** command.



Note CDP over Ethernet/radio interfaces is available only when CDP is enabled. After you enable CDP on all access points joined to the controller, you may disable and then reenabling CDP on individual access points using the **config ap cdp {enable | disable} cisco_ap** command. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.

The following example shows how to enable CDP on all access points:

```
(Cisco Controller) >config ap cdp enable all
```

The following example shows how to disable CDP on ap02 access point:

```
(Cisco Controller) >config ap cdp disable ap02
```

The following example shows how to enable CDP for Ethernet interface number 2 on all access points:

```
(Cisco Controller) >config ap cdp ethernet 2 enable all
```

config ap cert-expiry-ignore

To configure the device certificate date validation check, use the **config ap cert-expiry-ignore** command.

config ap cert-expiry-ignore { mic | ssc { enable | disable } }

Syntax Description

cert-expiry-ignore	Configures certificate expiry-ignore check operation.
mic	Configures cert-expiry-ignore check operation for MIC.
ssc	Configures cert-expiry-ignore check operation for SSC.
enable	Enabling will ignore the lifetime-check.
disable	Disabling will do the lifetime-check.

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.7	This command was enhanced to include certificate date validation check for the controller.

The following example shows how to ignore lifetime check on MIC certificate:

```
(Cisco Controller) >config ap cert-expiry-ignore mic enable
```

config ap core-dump

To configure a Cisco lightweight access point's memory core dump, use the **config ap core-dump** command.

```
config ap core-dump { disable | enable tftp_server_ipaddress filename { compress | uncompress }  
{ cisco_ap | all }
```

Syntax Description		
enable		Enables the Cisco lightweight access point's memory core dump setting.
disable		Disables the Cisco lightweight access point's memory core dump setting.
<i>tftp_server_ipaddress</i>		IP address of the TFTP server to which the access point sends core dump files.
<i>filename</i>		Name that the access point uses to label the core file.
compress		Compresses the core dump file.
uncompress		Uncompresses the core dump file.
<i>cisco_ap</i>		Name of a Cisco lightweight access point.
all		Specifies all access points.



Note If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

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 both IPv4 and IPv6.

Usage Guidelines The access point must be able to reach the TFTP server. This command is applicable for both IPv4 and IPv6 addresses.

The following example shows how to configure and compress the core dump file:

```
(Cisco Controller) >config ap core-dump enable 209.165.200.225 log compress AP02
```

config ap crash-file clear-all

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

config ap crash-file clear-all

Syntax Description	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 delete all crash files:

```
(Cisco Controller) >config ap crash-file clear-all
```

config ap crash-file delete

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

config ap crash-file delete *filename*

Syntax Description	<i>filename</i>	Name of the file to delete.
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 crash file 1:

```
(Cisco Controller) >config ap crash-file delete crash_file_1
```

config ap crash-file get-crash-file

To collect the latest crash data for a Cisco lightweight access point, use the **config ap crash-file get-crash-file** command.

config ap crash-file get-crash-file *cisco_ap*

Syntax Description	<i>cisco_ap</i>	Name of the Cisco lightweight 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	Use the transfer upload datatype command to transfer the collected data to the Cisco wireless LAN controller.	

The following example shows how to collect the latest crash data for access point AP3:

```
(Cisco Controller) >config ap crash-file get-crash-file AP3
```

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

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

config ap crash-file get-radio-core-dump *slot_id* *cisco_ap*

Syntax Description	<i>slot_id</i>	Slot ID (either 0 or 1).
	<i>cisco_ap</i>	Name of a Cisco lightweight 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 example shows how to collect the radio core dump for access point AP02 and slot 0:

```
(Cisco Controller) >config ap crash-file get-radio-core-dump 0 AP02
```

config ap dhcp release-override

To configure DHCP release override on Cisco APs, use the **config ap dhcp release-override** command.

config ap dhcp release-override {**enable** | **disable**} {*cisco-ap-name* | **all**}

Syntax Description	enable	Enables DHCP release override and sets number of DHCP releases sent by AP to 1. To be used as a workaround for a few DHCP servers that mark the AP's IP address as bad. We recommend that you use this configuration only in highly reliable networks.	
	disable	Disables DHCP release override and sets number of DHCP releases sent by AP to 3, which is the default value. This ensures that the DHCP server receives the release message even if one of the packets is lost.	
	cisco-ap-name	Configuration is applied to the Cisco AP that you enter	
	all	Configuration is applied to all Cisco APs	
Command Default	Disabled		
Command History	Release	Modification	
	8.2	This command was introduced.	
Usage Guidelines	Use this command when you are using Cisco lightweight APs with Windows Server 2008 R2 or 2012 as the DHCP server.		

config ap dtls-cipher-suite

To enable new cipher suites for DTLS connection between AP and controller, use the **config ap dtls-cipher-suite** command.

```
config ap dtls-cipher-suite { RSA-AES256-SHA256 | RSA-AES256-SHA | RSA-AES128-SHA }
```

Syntax Description	RSA-AES256-SHA256	Cipher suite using either RSA key exchange or authentication, using 256 bit AES and SHA 256.
	RSA-AES256-SHA	Cipher suite using either RSA key exchange or authentication, using 256 bit AES and SHA.
	RSA-AES128-SHA	Cipher suite using either RSA key exchange or authentication, using 128 bit AES and SHA.
Command Default	None	
Command History	Release	Modification
	8.0	This command was introduced.

The following example shows how to enable RSA cipher suites using 256 bit AES and SHA 256 for DTLS connection between AP and controller:

```
(Cisco Controller) >config ap dtls-cipher-suite RSA-AES256-SHA256
```

config ap dtls-version

To configure the cipher DTLS version, use the **config ap dtls-version** command.

config ap dtls-version { dtls1.0 | dtls1.2 | dtls_all }

Syntax Description	dtls1.0	Select DTLS 1.0 version
	dtls1.2	Select DTLS 1.2 version
	dtls_all	Select all DTLS versions for backward compatibility

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

Command History	Release	Modification
	8.3.111.0	This command was introduced.

The following example shows how to configure cipher dtls version 1.2:

```
(Cisco Controller) > config ap dtls-version dtls1.2
```

config ap ethernet duplex

To configure the Ethernet port duplex and speed settings of the lightweight access points, use the **config ap ethernet duplex** command.

config ap ethernet duplex [**auto** | **half** | **full**] **speed** [**auto** | **10** | **100** | **1000**] { **all** | *cisco_ap* }

Syntax Description	auto	(Optional) Specifies the Ethernet port duplex auto settings.
	half	(Optional) Specifies the Ethernet port duplex half settings.
	full	(Optional) Specifies the Ethernet port duplex full settings.
	speed	Specifies the Ethernet port speed settings.
	auto	(Optional) Specifies the Ethernet port speed to auto.
	10	(Optional) Specifies the Ethernet port speed to 10 Mbps.
	100	(Optional) Specifies the Ethernet port speed to 100 Mbps.
	1000	(Optional) Specifies the Ethernet port speed to 1000 Mbps.
	all	Specifies the Ethernet port setting for all connected access points.
	<i>cisco_ap</i>	Cisco 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 example shows how to configure the Ethernet port duplex half settings as 10 Mbps for all access points:

```
(Cisco Controller) >config ap ethernet duplex half speed 10 all
```

config ap ethernet tag

To configure VLAN tagging of the Control and Provisioning of Wireless Access Points protocol (CAPWAP) packets, use the **config ap ethernet tag** command.

config ap ethernet tag {**id** *vlan_id* | **disable**} {*cisco_ap* | **all**}

Syntax Description	id	Specifies the VLAN id.
	<i>vlan_id</i>	ID of the trunk VLAN.
	disable	Disables the VLAN tag feature. When you disable VLAN tagging, the access point untags the CAPWAP packets.
	<i>cisco_ap</i>	Name of the Cisco AP.
	all	Configures VLAN tagging on all the Cisco 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	After you configure VLAN tagging, the configuration comes into effect only after the access point reboots. You cannot configure VLAN tagging on mesh access points.
	If the access point is unable to route traffic or reach the controller using the specified trunk VLAN, it falls back to the untagged configuration. If the access point joins the controller using this fallback configuration, the controller sends a trap to a trap server such as the Cisco Prime Infrastructure, which indicates the failure of the trunk VLAN. In this scenario, the "Failover to untagged" message appears in show command output.

The following example shows how to configure VLAN tagging on a trunk VLAN:

```
(Cisco Controller) >config ap ethernet tag 6 AP1
```

config ap autoconvert

To automatically convert all access points to FlexConnect mode or Monitor mode upon associating with the controller, use the **config ap autoconvert** command.

config ap autoconvert { **flexconnect** | **monitor** | **disable** }

Syntax Description	flexconnect	Configures all the access points automatically to FlexConnect mode.
	monitor	Configures all the access points automatically to monitor mode.
	disable	Disables the autoconvert option on the 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

When access points in local mode connect to a Cisco 7500 Series Wireless Controller, they do not serve clients. The access point details are available in the controller. To enable access points to serve clients or perform monitoring related tasks when connected to the Cisco 7500 Series Wireless Controller, the access points must be in FlexConnect mode or Monitor mode.

The command can also be used for conversion of AP modes in Cisco 5520, 8540, and 8510 Series Wireless Controller platforms.

The following example shows how to automatically convert all access points to the FlexConnect mode:

```
(Cisco Controller) >config ap autoconvert flexconnect
```

The following example shows how to disable the autoconvert option on the APs:

```
(Cisco Controller) >config ap autoconvert disable
```

config ap flexconnect central-dhcp

To enable central-DHCP on a FlexConnect access point in a WLAN, use the **config ap flexconnect central-dhcp** command.

config ap flexconnect central-dhcp *wlan_id cisco_ap* [**add** | **delete**] {**enable** | **disable**} **override dns** {**enable** | **disable**} **nat-pat** {**enable** | **disable**}

Syntax Description	<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.
	add	(Optional) Adds a new WLAN DHCP mapping.
	delete	(Optional) Deletes a WLAN DHCP mapping.
	enable	Enables central-DHCP on a FlexConnect access point. When you enable this feature, the DHCP packets received from the access point are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.
	disable	Disables central-DHCP on a FlexConnect access point.
	override dns	Overrides the DNS server address on the interface assigned by the controller. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP and not from the controller.
	enable	Enables the Override DNS feature on a FlexConnect access point.
	disable	Disables the Override DNS feature on a FlexConnect access point.
	nat-pat	Network Address Translation (NAT) and Port Address Translation (PAT) that you can enable or disable.
	enable	Enables NAT-PAT on a FlexConnect access point.
	disable	Deletes NAT-PAT on a FlexConnect 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 example shows how to enable central-DHCP, Override DNS, and NAT-PAT on a FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect central-dhcp 1 ap1250 enable override dns enable nat-pat enable
```

config ap flexconnect local-split

To configure a local-split tunnel on a FlexConnect access point, use the **config ap flexconnect local-split** command.

config ap flexconnect local-split *wlan_id* *cisco_ap* {**enable** | **disable**} **acl** *acl_name*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>cisco_ap</i>	Name of the FlexConnect access point.
enable	Enables local-split tunnel on a FlexConnect access point.
disable	Disables local-split tunnel feature on a FlexConnect access point.
acl	Configures a FlexConnect local-split access control list.
<i>acl_name</i>	Name of the FlexConnect access control list.

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 allows you to configure a local-split tunnel in a centrally switched WLAN using a FlexConnect ACL. A local split tunnel supports only for unicast Layer 4 IP traffic as NAT/PAT does not support multicast IP traffic.

The following example shows how to configure a local-split tunnel using a FlexConnect ACL:

```
(Cisco Controller) >config ap flexconnect local-split 6 AP2 enable acl flex6
```

config ap flexconnect module-vlan

To configure VLAN tagging for Cisco USC 8x18 Dual Mode Module in FlexConnect Local Switching, use the **config ap flexconnect module-vlan** command.

```
config ap flexconnect module-vlan { {enable ap-name [vlan vlan-id] } | { {disable | remove} ap-name } }
```

Syntax Description	enable <i>ap-name</i>	Enables FlexConnect local switching for the external module of the specified Cisco AP with native VLAN
	enable <i>ap-name</i> vlan <i>vlan-id</i>	Enables FlexConnect local switching with non-native VLAN for the external module of the specified Cisco AP
	disable <i>ap-name</i>	Disables FlexConnect local switching for the external module of the specified Cisco AP
	remove <i>ap-name</i>	Removes the AP-specific external module VLAN configuration

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

Command History	Release	Modification
	8.1	This command was introduced.

This example shows how to enable FlexConnect local switching with non-native VLAN for the external module of a Cisco AP:

```
(Cisco Controller) >config ap flexconnect module-vlan enable 3600i-ap vlan4
```


config ap flexconnect policy

To configure a policy ACL on a FlexConnect access point, use the **config ap flexconnect policy** command.

config ap flexconnect policy {**add** | **delete**} *acl_name*

Syntax Description	add	Adds a policy ACL on a FlexConnect access point.
	deletes	Deletes a policy ACL on a FlexConnect access point.
	<i>acl_name</i>	Name of the ACL.

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

Command History	Release	Modification
	7.5	This command was introduced.

The following example shows how to add a policy ACL on a FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect policy add acl1
```

config ap flexconnect radius auth set

To configure a primary or secondary RADIUS server for a specific FlexConnect access point, use the **config ap flexconnect radius auth set** command.

config ap flexconnect radius auth set {**primary** | **secondary**} *ip_address auth_port secret*

Syntax Description	primary	Specifies the primary RADIUS server for a specific FlexConnect access point
	secondary	Specifies the secondary RADIUS server for a specific FlexConnect AP
	<i>ip_address</i>	IP address of the RADIUS server
	<i>auth_port secret</i>	Name of the port
	<i>secret</i>	RADIUS server secret
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 primary RADIUS server for a specific access point:

```
(Cisco Controller) >config ap flexconnect radius auth set primary 192.12.12.1
```

config ap flexconnect vlan

To enable or disable VLAN tagging for a FlexConnect access, use the **config ap flexconnect vlan** command.

```
config ap flexconnect vlan { enable | disable } cisco_ap
```

Syntax Description	enable	Enables the access point's VLAN tagging.
	disable	Disables the access point's VLAN tagging.
	cisco_ap	Name of the Cisco lightweight access point.
Command Default	Disabled. Once enabled, WLANs enabled for local switching inherit the VLAN assigned at the controller.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to enable the access point's VLAN tagging for a FlexConnect access:

```
(Cisco Controller) >config ap flexconnect vlan enable AP02
```

config ap flexconnect vlan add

To add a VLAN to a FlexConnect access point, use the **config ap flexconnect vlan add** command.

config ap flexconnect vlan add *vlan-id acl in-acl out-acl cisco_ap*

Syntax Description	<i>vlan-id</i>	VLAN identifier.
	<i>acl</i>	ACL name that contains up to 32 alphanumeric characters.
	<i>in-acl</i>	Inbound ACL name that contains up to 32 alphanumeric characters.
	<i>out-acl</i>	Outbound ACL name that contains up to 32 alphanumeric characters.
	<i>cisco_ap</i>	Name of the Cisco lightweight 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 example shows how to configure the FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect vlan add 21 acl inacl1 outacl1 ap1
```

config ap flexconnect vlan native

To configure a native VLAN for a FlexConnect access point, use the **config ap flexconnect vlan native** command.

config ap flexconnect vlan native *vlan-id cisco_ap*

Syntax Description	<i>vlan-id</i>	VLAN identifier.
	<i>cisco_ap</i>	Name of the Cisco lightweight 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 example shows how to configure a native VLAN for a FlexConnect access point mode:

```
(Cisco Controller) >config ap flexconnect vlan native 6 AP02
```

config ap flexconnect vlan wlan

To assign a VLAN ID to a FlexConnect access point, use the **config ap flexconnect vlan wlan** command.

config ap flexconnect vlan wlan *wlan-id* *vlan-id* *cisco_ap*

Syntax Description	<i>wlan-id</i>	WLAN identifier
	<i>vlan-id</i>	VLAN identifier (1 - 4094).
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.
Command Default	VLAN ID associated to the WLAN.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to assign a VLAN ID to a FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect vlan wlan 192.12.12.1 6 AP02
```

config ap flexconnect web-auth

To configure a FlexConnect ACL for external web authentication in locally switched WLANs, use the **config ap flexconnect web-auth** command.

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

Syntax Description	wlan	Specifies the wireless LAN to be configured with a FlexConnect ACL.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512 (inclusive).
	<i>cisco_ap</i>	Name of the FlexConnect access point.
	<i>acl_name</i>	Name of the FlexConnect ACL.
	enable	Enables the FlexConnect ACL on the locally switched wireless LAN.
	disable	Disables the FlexConnect ACL on the locally switched wireless LAN.
Command Default	FlexConnect ACL for external web authentication in locally switched WLANs is disabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	The FlexConnect ACLs that are specific to an AP have the highest priority. The FlexConnect ACLs that are specific to WLANs have the lowest priority.	
	The following example shows how to enable FlexConnect ACL for external web authentication on WLAN 6: (Cisco Controller) > config ap flexconnect web-auth wlan 6 AP2 flexacl2 enable	

config ap flexconnect web-policy acl

To configure a Web Policy FlexConnect ACL on an access point, use the **config ap flexconnect web-policy acl** command.

config ap flexconnect web-policy acl { **add** | **delete** } *acl_name*

Syntax Description	add	Adds a Web Policy FlexConnect ACL on an access point.
	delete	Deletes Web Policy FlexConnect ACL on an access point.
	<i>acl_name</i>	Name of the Web Policy FlexConnect 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 a Web Policy FlexConnect ACL on an access point:

```
(Cisco Controller) >config ap flexconnect web-policy acl add flexacl2
```


config ap flexconnect wlan

To configure a FlexConnect access point in a locally switched WLAN, use the **config ap flexconnect wlan** command.

```
config ap flexconnect wlan l2acl { add wlan_id cisco_ap acl_name | delete wlan_id cisco_ap }
```

Syntax Description	add	Adds a Layer 2 ACL to the FlexConnect access point.
	wlan_id	Wireless LAN identifier from 1 to 512.
	cisco_ap	Name of the Cisco lightweight access point.
	acl_name	Layer 2 ACL name. The name can be up to 32 alphanumeric characters.
	delete	Deletes a Layer 2 ACL from the FlexConnect access point.
Command Default	None	
Command History	Release	Modification
	7.5	This command was introduced.
Usage Guidelines	<ul style="list-style-type: none"> 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 controller. A maximum of 16 Layer 2 ACLs are supported per AP because an AP supports a maximum of 16 WLANs. Ensure that the Layer 2 ACL names do not conflict with the FlexConnect ACL names because an AP does not support the same Layer 2 and Layer 3 ACL names. 	

The following example shows how to configure a Layer 2 ACL on a FlexConnect AP.

```
(Cisco Controller) >config ap flexconnect wlan add 1 AP1600_1 acl_12_1
```

config ap group-name

To specify a descriptive group name for a Cisco lightweight access point, use the **config ap group-name** command.

config ap group-name *groupname* *cisco_ap*

Syntax Description	<i>groupname</i>	Descriptive name for the access point group.
	<i>cisco_ap</i>	Name of the Cisco lightweight 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	The Cisco lightweight access point must be disabled before changing this parameter.	

The following example shows how to configure a descriptive name for access point AP01:

(Cisco Controller) >**config ap group-name superusers AP01**

config ap hotspot

To configure hotspot parameters on an access point, use the **config ap hotspot** command.

```
config ap hotspot venue { type group_code type_code | name { add language_code venue_name | delete } } cisco_ap
```

Syntax Description	
venue	Configures venue information for given AP group.
type	Configures the type of venue for given AP group.
group_code	<p>Venue group information for given AP group.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> • 0—UNSPECIFIED • 1—ASSEMBLY • 2—BUSINESS • 3—EDUCATIONAL • 4—FACTORY-INDUSTRIAL • 5—INSTITUTIONAL • 6—MERCANTILE • 7—RESIDENTIAL • 8—STORAGE • 9—UTILITY-MISC • 10—VEHICULAR • 11—OUTDOOR

type_code

Venue type information for the 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
-

type_code

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 option is:

- 0—UNSPECIFIED STORAGE

For venue group 9 (UTILITY-MISC), the option is:

- 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

name	Configures the name of venue for this access point.
<i>language_code</i>	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 access point. 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.
add	Adds the HotSpot venue name for this access point.
delete	Deletes the HotSpot venue name for this access point.
<i>cisco_ap</i>	Name of the Cisco 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 example shows how to configure the venue group as educational and venue type as university:

```
(Cisco Controller) >config ap hotspot venue type 3 3
```

config ap image predownload

To configure an image on a specified access point, use the **config ap image predownload** command.

config ap image predownload {**abort** | **primary** | **backup**} {*cisco_ap* | **all**}

Syntax Description

abort	Terminates the predownload image process.
primary	Predownloads an image to a Cisco access point from the controller's primary image.
<i>cisco_ap</i>	Name of a Cisco lightweight access point.
all	Specifies all access points to predownload an image.

(Cisco Controller) >



Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

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 predownload an image to an access point from the primary image:

```
(Cisco Controller) >config ap image predownload primary all
```

config ap image swap

To swap an access point’s primary and backup images, use the **config ap image swap** command.

config ap image swap { *cisco_ap* | **all** }

Syntax Description	<i>cisco_ap</i>	Name of a Cisco lightweight access point.
	all	Specifies all access points to interchange the boot images.



Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

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 swap an access point’s primary and secondary images:

(Cisco Controller) >**config ap image swap all**

config ap ipsla

To configure the IP Service Level Agreements of the AP, use the **config ap ipsla** command.

```
config ap ipsla { enable | disable } ap_name
```

Syntax Description	Enable	Enables IPSLA on an AP.
	Disable	Disables IPSLA 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 IPSLA on an AP:

```
(Cisco Controller) > config ap ipsla cz2340212
```

config ap led-state

To configure the LED state of an access point or to configure the flashing of LEDs, use the **config ap led-state** command.

config ap led-state {enable | disable} {cisco_ap | all}

config ap led-state flash {seconds | indefinite | disable} {cisco_ap | dual-band}

Syntax Description	enable	Enables the LED state of an access point.
	disable	Disables the LED state of an access point.
	<i>cisco_ap</i>	Name of a Cisco lightweight access point.
	flash	Configure the flashing of LEDs for an access point.
	<i>seconds</i>	Duration that the LEDs have to flash. The range is from 1 to 3600 seconds.
	indefinite	Configures indefinite flashing of the access point's LED.
	dual-band	Configures the LED state for all dual-band access points.

Usage Guidelines



Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

LEDs on access points with dual-band radio module will flash green and blue when you execute the led state flash command.

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 LED state for an access point:

```
(Cisco Controller) >config ap led-state enable AP02
```

The following example shows how to enable the flashing of LEDs for dual-band access points:

```
(Cisco Controller) >config ap led-state flash 20 dual-band
```

config ap link-encryption

To configure the Datagram Transport Layer Security (DTLS) data encryption for access points on the 5500 series controller, use the **config ap link-encryption** command.



Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

config ap link-encryption {**enable** | **disable**} {*cisco_ap* | **all**}

Syntax Description

enable Enables the DTLS data encryption for access points.

disable Disables the DTLS data encryption for access points.

cisco_ap Name of a Cisco lightweight access point.

all Specifies all access points.

Command Default

DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points.

Command History

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

Usage Guidelines

Only Cisco 5500 Series Controllers support DTLS data encryption. This feature is not available on other controller platforms. If an access point with data encryption enabled tries to join any other controller, the access point joins the controller, but data packets are sent unencrypted.

Only Cisco 1130, 1140, 1240, and 1250 series access points support DTLS data encryption, and data-encrypted access points can join a Cisco 5500 Series Controller only if the wplus license is installed on the controller. If the wplus license is not installed, the access points cannot join the controller.

The following example shows how to enable the data encryption for an access point:

```
(Cisco Controller) >config ap link-encryption enable AP02
```

config ap link-latency

To configure link latency for a specific access point or for all access points currently associated to the controller, use the **config ap link-latency** command:



Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

config ap link-latency {**enable** | **disable** | **reset**} {*cisco_ap* | **all**}

Syntax Description	enable	Enables the link latency for an access point.
	disable	Disables the link latency for an access point.
	reset	Resets all link latency for all access points.
	<i>cisco_ap</i>	Name of the Cisco lightweight access point.
	all	Specifies all access points.

Command Default By default, link latency is in disabled state.

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

Usage Guidelines This command enables or disables link latency only for access points that are currently joined to the controller. It does not apply to access points that join in the future.

The following example shows how to enable the link latency for all access points:

```
(Cisco Controller) >config ap link-latency enable all
```

config ap location

To modify the descriptive location of a Cisco lightweight access point, use the **config ap location** command.

config ap location *location cisco_ap*

Syntax Description	<i>location</i>	Location name of the access point (enclosed by double quotation marks).
	<i>cisco_ap</i>	Name of the Cisco lightweight 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	The Cisco lightweight access point must be disabled before changing this parameter.	

The following example shows how to configure the descriptive location for access point AP1:

```
(Cisco Controller) >config ap location "Building 1" AP1
```


config ap logging syslog level

To set the severity level for filtering syslog messages for a particular access point or for all access points, use the **config ap logging syslog level** command.

config ap logging syslog level *severity_level* { *cisco_ap* | **all** }

Syntax Description		
<i>severity_level</i>		Severity levels are as follows: <ul style="list-style-type: none"> • emergencies—Severity level 0 • alerts—Severity level 1 • critical—Severity level 2 • errors—Severity level 3 • warnings—Severity level 4 • notifications—Severity level 5 • informational—Severity level 6 • debugging—Severity level 7
<i>cisco_ap</i>		Cisco access point.
all		Specifies all access points.



Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

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 set a syslog level, only those messages whose severity is equal to or less than that level are sent to the access point. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the access point.

This example shows how to set the severity for filtering syslog messages to 3:

```
(Cisco Controller) >config ap logging syslog level 3
```

config ap logging syslog facility

To set the facility level for filtering syslog messages for a particular access point or for all access points, use the **config ap logging syslog facility** command.

config ap logging syslog facility *facility-level* { *cisco_ap* | **all** }

Syntax Description

facility-level

Facility level is one of the following:

- auth = Authorization system.
 - cron = Cron/at facility.
 - daemon = System daemons.
 - kern = Kernel.
 - local0 = Local use.
 - local1 = Local use.
 - local2 = Local use.
 - local3 = Local use.
 - local4 = Local use.
 - local5 = Local use.
 - local5 = Local use.
 - local6 = Local use.
 - local7 = Local use.
 - lpr = Line printer system.
 - mail = Mail system.
 - news = USENET news.
 - sys10 = System use.
 - sys11 = System use.
 - sys12 = System use.
 - sys13 = System use.
 - sys14 = System use.
 - sys9 = System use.
 - syslog = Syslog itself.
 - user = User process.
 - uucp Unix-to-Unix copy system.
-

<i>cisco_ap</i>	Configures for a specific access point.
-----------------	---

all	Configures for all access points.
------------	-----------------------------------

Command Default

None

Command History

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

This example shows how to set the facility level for filtering syslog messages to auth for all access points:

```
(Cisco Controller) >config ap logging syslog facility auth all
```

config ap max-count

To configure the maximum number of access points supported by the controller, use the **config ap max-count** command.

config ap max-count *number*

Syntax Description

number Number of access points supported by the controller.

Command Default

None

Command History

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

Usage Guidelines

The access point count of the controller license overrides this count if the configured value is greater than the access point count of the license. A value of 0 indicates that there is no restriction on the maximum number of access points. If high availability is configured, you must reboot both the active and the standby controllers after you configure the maximum number of access points supported by the controller.

The following example shows how to configure the number of access points supported by the controller:

```
(Cisco Controller) >config ap max-count 100
```

config ap mgmtuser add

To configure username, password, and secret password for AP management, use the **config ap mgmtuser add** command.

config ap mgmtuser add username *AP_username* **password** *AP_password* **secret** *secret* { **all** | *cisco_ap* }

Syntax Description		
username		Configures the username for AP management.
<i>AP_username</i>		Management username.
password		Configures the password for AP management.
<i>AP_password</i>		AP management password.
secret		Configures the secret password for privileged AP management.
<i>secret</i>		AP management secret password.
all		Applies configuration to every AP that does not have a specific username.
<i>cisco_ap</i>		Cisco 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	<p>The following requirements are enforced on the password:</p> <ul style="list-style-type: none"> • The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters. • No character in the password can be repeated more than three times consecutively. • The password should not contain management username or reverse of username. • The password should not contain words like Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting l, , or ! or substituting 0 for o or substituting \$ for s. <p>The following requirement is enforced on the secret password:</p> <ul style="list-style-type: none"> • The secret password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, or special characters.
------------------	--

The following example shows how to add a username, password, and secret password for AP management:

```
(Cisco Controller) > config ap mgmtuser add username acd password Arc_1234 secret Mid_45
all
```

config ap mgmtuser delete

To force a specific access point to use the controller’s global credentials, use the **config ap mgmtuser delete** command.

config ap mgmtuser delete *cisco_ap*

Syntax Description	<i>cisco_ap</i>	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 example shows how to delete the credentials of an access point:

```
(Cisco Controller) > config ap mgmtuser delete cisco_ap1
```

config ap mode

To change a controller communication option for an individual Cisco lightweight access point, use the **config ap mode** command.

```
config ap mode {bridge | flexconnect submode {none | wips} | local submode {none | wips} | reap | rogue | sniffer | se-connect | monitor submode {none | wips} | }
cisco_ap
```

Syntax Description		
bridge		Converts from a lightweight access point to a mesh access point (bridge mode).
flexconnect		Enables FlexConnect mode on an access point.
local		Converts from an indoor mesh access point (MAP or RAP) to a non-mesh lightweight access point (local mode).
reap		Enables remote edge access point mode on an access point.
rogue		Enables wired rogue detector mode on an access point.
sniffer		Enables wireless sniffer mode on an access point.
se-connect		Enables flex+bridge mode on an access point.
flex+bridge		Enables spectrum expert mode on an access point.
submode		(Optional) Configures wIPS submode on an access point.
none		Disables the wIPS on an access point.
wips		Enables the wIPS submode on an access point.
<i>cisco_ap</i>		Name of the Cisco lightweight access point.

Command Default	Local
------------------------	-------

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

Usage Guidelines

The sniffer mode captures and forwards all the packets from the clients on that channel to a remote machine that runs AiroPeek or other supported packet analyzer software. It includes information on the timestamp, signal strength, packet size and so on.

The following example shows how to set the controller to communicate with access point AP91 in bridge mode:

```
(Cisco Controller) > config ap mode bridge AP91
```

The following example shows how to set the controller to communicate with access point AP01 in local mode:

```
(Cisco Controller) > config ap mode local AP01
```

The following example shows how to set the controller to communicate with access point AP91 in remote office (REAP) mode:

```
(Cisco Controller) > config ap mode flexconnect AP91
```

The following example shows how to set the controller to communicate with access point AP91 in a wired rogue access point detector mode:

```
(Cisco Controller) > config ap mode rogue AP91
```

The following example shows how to set the controller to communicate with access point AP02 in wireless sniffer mode:

```
(Cisco Controller) > config ap mode sniffer AP02
```


config ap module3g

To configure the Cisco Universal Small Cell (USC) 8x18 Dual Mode Module, use the **config ap module3g** command.

config ap module3g {**enable** | **disable**} *ap-name*

Syntax Description	enable	Enables the Cisco USC 8x18 Dual Mode Module on the specified Cisco AP.
	disable	Disables the Cisco USC 8x18 Dual Mode Module on the specified Cisco AP.
	<i>ap-name</i>	Name of the Cisco AP
	Note	In Release 8.1, only Cisco Aironet 3600I and 3700I APs are supported.
Command Default	Enabled	
Command History	Release	Modification
	8.1	This command was introduced.
Usage Guidelines	You might be prompted with a co-existence warning when Wi-Fi in 2.4-GHz and 3G/4G module are enabled.	
	This example shows how to enable Cisco USC 8x18 Dual Mode Module on a Cisco AP named <i>my-ap</i> (Cisco Controller) > config ap module3g enable my-ap	

config ap monitor-mode

To configure Cisco lightweight access point channel optimization, use the **config ap monitor-mode** command.

```
config ap monitor-mode {802.11b fast-channel | no-optimization | tracking-opt | wips-optimized}
cisco_ap
```

Syntax Description	802.11b fast-channel	Configures 802.11b scanning channels for a monitor-mode access point.
	no-optimization	Specifies no channel scanning optimization for the access point.
	tracking-opt	Enables tracking optimized channel scanning for the access point.
	wips-optimized	Enables WIPS optimized channel scanning for the access point.
	cisco_ap	Name of the Cisco lightweight 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 example shows how to configure a Cisco wireless intrusion prevention system (WIPS) monitor mode on access point AP01:

```
(Cisco Controller) > config ap monitor-mode wips-optimized AP01
```

config ap name

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

config ap name *new_name old_name*

Syntax Description	<i>new_name</i>	Desired Cisco lightweight access point name.
	<i>old_name</i>	Current Cisco lightweight access point 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 modify the name of access point AP1 to AP2:

```
(Cisco Controller) > config ap name AP1 AP2
```

config ap packet-dump

To configure the Packet Capture parameters on access points, use the **config ap packet-dump** command.

```
config ap packet-dump {buffer-size Size_in_KB | capture-time Time_in_Min | ftp serverip IP_addr
path path username username password password | start MAC_address Cisco_AP | stop | truncate
Length_in_Bytes}
config ap packet-dump classifier {{arp | broadcast | control | data | dot1x | iapp | ip |
management | multicast } {enable | disable} | tcp {enable | disable | port TCP_Port {enable
| disable}} | udp {enable | disable | port UDP_Port {enable | disable}}}
```

Syntax Description

buffer-size	Configures the buffer size for Packet Capture in the access point.
<i>Size_in_KB</i>	Size of the buffer. The range is from 1024 to 4096 KB.
capture-time	Configures the timer value for Packet Capture.
<i>Time_in_Min</i>	Timer value for Packet Capture. The range is from 1 to 60 minutes.
ftp	Configures FTP parameters for Packet Capture.
serverip	Configures the FTP server.
<i>IP_addr</i>	IP address of the FTP server.
path <i>path</i>	Configures FTP server path.
username <i>user_ID</i>	Configures the username for the FTP server.
password <i>password</i>	Configures the password for the FTP server.
start	Starts Packet Capture from the access point.
<i>MAC_address</i>	Client MAC Address for Packet Capture.
<i>Cisco_AP</i>	Name of the Cisco access point.
stop	Stops Packet Capture from the access point.
truncate	Truncates the packet to the specified length during Packet Capture.

<i>Length_in_Bytes</i>	Length of the packet after truncation. The range is from 20 to 1500.
classifier	Configures the classifier information for Packet Capture. You can specify the type of packets that needs to be captured.
arp	Captures ARP packets.
enable	Enables capture of ARP, broadcast, 802.11 control, 802.11 data, dot1x, Inter Access Point Protocol (IAPP), IP, 802.11 management, or multicast packets.
disable	Disables capture of ARP, broadcast, 802.11 control, 802.11 data, dot1x, IAPP, IP, 802.11 management, or multicast packets.
broadcast	Captures broadcast packets.
control	Captures 802.11 control packets.
data	Captures 802.11 data packets.
dot1x	Captures dot1x packets.
iapp	Captures IAPP packets.
ip	Captures IP packets.
management	Captures 802.11 management packets.
multicast	Captures multicast packets.
tcp	Captures TCP packets.
<i>TCP_Port</i>	TCP port number. The range is from 1 to 65535.
udp	Captures UDP packets.
<i>UDP_Port</i>	UDP port number. The range is from 1 to 65535.
ftp	Configures FTP parameters for Packet Capture.
<i>server_ip</i>	FTP server IP address.

Command Default

The default buffer size is 2 MB. The default capture time is 10 minutes.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.
8.8	This command is not supported for Cisco Wave 2 APs. For more information, see CSCvj19314 .

Usage Guidelines

Packet Capture does not work during intercontroller roaming.

The controller does not capture packets created in the radio firmware and sent out of the access point, such as a beacon or probe response. Only packets that flow through the Radio driver in the Tx path will be captured.

Use the command **config ap packet-dump start** to start the Packet Capture from the access point. When you start Packet Capture, the controller sends a Control and Provisioning of Wireless Access Points protocol (CAPWAP) message to the access point to which the client is associated and captures packets. You must configure the FTP server and ensure that the client is associated to the access point before you start Packet Capture. If the client is not associated to the access point, you must specify the name of the access point.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to start Packet Capture from an access point:

```
(Cisco Controller) >config ap packet-dump start 00:0d:28:f4:c0:45 AP1
```

The following example shows how to capture 802.11 control packets from an access point:

```
(Cisco Controller) >config ap packet-dump classifier control enable
```

config ap port

To configure the port for a foreign access point, use the **config ap port** command.

config ap port *MAC port*

Syntax Description	<i>MAC</i>	Foreign access point MAC address.
	<i>port</i>	Port number for accessing the foreign 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 example shows how to configure the port for a foreign access point MAC address:

```
(Cisco Controller) > config ap port 12:12:12:12:12:12 20
```

config ap power injector

To configure the power injector state for an access point, use the **config ap power injector** command.

config ap power injector {**enable** | **disable**} {*cisco_ap* | **all**} {**installed** | **override** | *switch_MAC*}

Syntax	Description
enable	Enables the power injector state for an access point.
disable	Disables the power injector state for an access point.
<i>cisco_ap</i>	Name of the Cisco lightweight access point.
all	Specifies all Cisco lightweight access points connected to the controller.
installed	Detects the MAC address of the current switch port that has a power injector.
override	Overrides the safety checks and assumes a power injector is always installed.
<i>switch_MAC</i>	MAC address of the switch port with an installed power injector.



Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

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 power injector state for all access points:

```
(Cisco Controller) > config ap power injector enable all 12:12:12:12:12:12
```


config ap power pre-standard

To enable or disable the inline power Cisco pre-standard switch state for an access point, use the **config ap power pre-standard** command.

```
config ap power pre-standard { enable | disable } cisco_ap
```

Syntax Description	enable	Enables the inline power Cisco pre-standard switch state for an access point.
	disable	Disables the inline power Cisco pre-standard switch state for an access point.
	cisco_ap	Name of the Cisco lightweight access point.
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 inline power Cisco pre-standard switch state for access point AP02:

```
(Cisco Controller) > config ap power pre-standard enable AP02
```

config ap preferred-mode

To configure the preferred mode, use the **config ap preferred-mode** command.

config appreferred-mode{ **ipv4** | **ipv6** | **any** } { *AP_name* | *Ap-group_name* | *all* }

Syntax Description

ipv4	Configures IPv4 as the preferred mode
ipv6	Configures IPv6 as the preferred mode
any	Configures any as the preferred mode
<i>AP_name</i>	Configures the preferred mode to the AP
<i>Ap-group_name</i>	Configures the preferred mode to the AP group members
<i>all</i>	Configures the preferred mode to all the APs

Command Default

None

Command History

Release	Modification
8.0	This command was introduced. It supports both IPv4 and IPv6.

Example

The following example shows how to configure IPv6 as the preferred mode to lightweight access point AP1

```
(Cisco Controller) >config ap preferred-mode ipv6 AP1
```

config ap primary-base

To set the Cisco lightweight access point primary controller, use the **config ap primary-base** command.

config ap primary-base *controller_name* *Cisco_AP* [*controller_ip_address*]

Syntax Description	<i>controller_name</i>	Name of the controller.
	<i>Cisco_AP</i>	Cisco lightweight access point name.
	<i>controller_ip_address</i>	(Optional) If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller.
	Note	For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.
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 both IPv4 and IPv6 address formats.
Usage Guidelines	The Cisco lightweight access point associates with this controller for all network operations and in the event of a hardware reset.	
	OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.	
	This command supports both IPv4 and IPv6 address formats.	
	The following example shows how to set an access point primary controller IPv4 address for an Cisco AP:	
	<pre>(Cisco Controller) > config ap primary-base SW_1 AP2 10.0.0.0</pre>	
	The following example shows how to set an access point primary controller IPv6 address for an Cisco AP:	
	<pre>(Cisco Controller) > config ap primary-base SW_1 AP2 2001:DB8:0:1::1</pre>	
Related Commands	show ap config general	

config ap priority

To assign a priority designation to an access point that allows it to reauthenticate after a controller failure by priority rather than on a first-come-until-full basis, use the **config ap priority** command.

config ap priority {1 | 2 | 3 | 4} *cisco_ap*

Syntax Description	1	Specifies low priority.
	2	Specifies medium priority.
	3	Specifies high priority.
	4	Specifies the highest (critical) priority.
	<i>cisco_ap</i>	Cisco lightweight access point name.

Command Default	1 - Low priority.
-----------------	-------------------

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

Usage Guidelines	In a failover situation, if the backup controller does not have enough ports to allow all the access points in the affected area to reauthenticate, it gives priority to higher-priority access points over lower-priority ones, even if it means replacing lower-priority access points.
------------------	---

The following example shows how to assign a priority designation to access point AP02 that allows it to reauthenticate after a controller failure by assigning a reauthentication priority 3:

```
(Cisco Controller) > config ap priority 3 AP02
```

config ap reporting-period

To reset a Cisco lightweight access point, use the **config ap reporting-period** command.

config ap reporting-period *period*

Syntax Description	<i>period</i>	Time period in seconds between 10 and 120.
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 reset an access point reporting period to 120 seconds:

```
> config ap reporting-period 120
```

config ap reset

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

config ap reset *cisco_ap*

Syntax Description	<i>cisco_ap</i>	Cisco lightweight access point 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 reset an access point:

```
(Cisco Controller) > config ap reset AP2
```

config ap retransmit interval

To configure the access point control packet retransmission interval, use the **config ap retransmit interval** command.

config ap retransmit interval *seconds* { **all** | *cisco_ap* }

Syntax Description	<i>seconds</i>	AP control packet retransmission timeout between 2 and 5 seconds.
	all	Specifies all access points.
	<i>cisco_ap</i>	Cisco lightweight access point 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 the retransmission interval for all access points globally:

```
(Cisco Controller) > config ap retransmit interval 4 all
```

config ap retransmit count

To configure the access point control packet retransmission count, use the **config ap retransmit count** command.

config ap retransmit count *count* { **all** | *cisco_ap* }

Syntax Description	<i>count</i>	Number of times control packet will be retransmitted. The range is from 3 to 8.
	all	Specifies all access points.
	<i>cisco_ap</i>	Cisco lightweight access point 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 the retransmission retry count for a specific access point:

```
(Cisco Controller) > config ap retransmit count 6 cisco_ap
```


config ap role

To specify the role of an access point in a mesh network, use the **config ap role** command.

```
config ap role {rootAP | meshAP} cisco_ap
```

Syntax Description	rootAP	Designates the mesh access point as a root access point (RAP).
	meshAP	Designates the mesh access point as a mesh access point (MAP).
	cisco_ap	Name of the Cisco lightweight access point.
Command Default	meshAP.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	Use the meshAP keyword if the access point has a wireless connection to the controller, or use the rootAP keyword if the access point has a wired connection to the controller. If you change the role of the AP, the AP will be rebooted.	

The following example shows how to designate mesh access point AP02 as a root access point:

```
(Cisco Controller) > config ap role rootAP AP02
Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

config ap rst-button

To configure the Reset button for an access point, use the **config ap rst-button** command.

```
config ap rst-button {enable | disable} cisco_ap
```

Syntax Description	enable	Enables the Reset button for an access point.
	disable	Disables the Reset button for an access point.
	cisco_ap	Name of the Cisco lightweight 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 example shows how to configure the Reset button for access point AP03:

```
(Cisco Controller) > config ap rst-button enable AP03
```

config ap secondary-base

To set the Cisco lightweight access point secondary controller, use the **config ap secondary-base** command.

config ap secondary-base *Controller_name* *Cisco_AP* [*Controller_IP_address*]

Syntax Description	<i>controller_name</i>	Name of the controller.
	<i>Cisco_AP</i>	Cisco lightweight access point name.
	<i>Controller_IP_address</i>	(Optional). If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller.
	Note	For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

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 both IPv4 and IPv6 address formats.

Usage Guidelines

The Cisco lightweight access point associates with this controller for all network operations and in the event of a hardware reset.

OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to set an access point secondary controller:

```
(Cisco Controller) > config ap secondary-base SW_1 AP2 10.0.0.0
```

The following example shows how to set an access point primary controller IPv6 address for an Cisco AP:

```
(Cisco Controller) > config ap secondary-base SW_1 AP2 2001:DB8:0:1::1
```

Related Commands **show ap config general**

config ap sniff

To enable or disable sniffing on an access point, use the **config ap sniff** command.

```
config ap sniff { 802.11a | 802.11b } { enable channel server_ip | disable } cisco_ap
```

Syntax Description	802.11a	Specifies the 802.11a network.
	802.11b	Specifies the 802.11b network.
	enable	Enables sniffing on an access point.
	channel	Channel to be sniffed.
	server_ip	IP address of the remote machine running Omnipeek, Airopeek,AirMagnet, or Wireshark software.
	disable	Disables sniffing on an access point.
	cisco_ap	Access point configured as the sniffer.

Command Default Channel 36.

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

Usage Guidelines

When the sniffer feature is enabled on an access point, it starts sniffing the signal on the given channel. It captures and forwards all the packets to the remote computer that runs Omnipeek, Airopeek, AirMagnet, or Wireshark software. It includes information on the timestamp, signal strength, packet size and so on.

Before an access point can act as a sniffer, a remote computer that runs one of the listed packet analyzers must be set up so that it can receive packets sent by the access point. After the Airopeek installation, copy the following .dll files to the location where airopeek is installed:

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

The following example shows how to enable the sniffing on the 802.11a an access point from the primary controller:

```
(Cisco Controller) > config ap sniff 80211a enable 23 11.22.44.55 AP01
```

config ap ssh

To enable Secure Shell (SSH) connectivity on an access point, use the **config ap ssh** command.

config ap ssh {**enable** | **disable** | **default**} *cisco_ap* | *all*

Syntax Description	enable	Enables the SSH connectivity on an access point.
	disable	Disables the SSH connectivity on an access point.
	default	Replaces the specific SSH configuration of an access point with the global SSH configuration.
	<i>cisco_ap</i>	Cisco access point name.
	<i>all</i>	All 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	<p>The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operation and in the event of a hardware reset.</p> <p>The following example shows how to enable SSH connectivity on access point Cisco_ap2:</p> <pre>> config ap ssh enable cisco_ap2</pre>	

config ap static-ip

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

```
config ap static-ip { enable Cisco_AP AP_IP_addr IP_netmask /prefix_length gateway | disable
Cisco_AP | add { domain { Cisco_AP | all } domain_name | nameserver { Cisco_AP | all }
nameserver-ip } | delete { domain | nameserver } { Cisco_AP | all } }
```

Syntax Description		
enable		Enables the Cisco lightweight access point static IP address.
disable		Disables the Cisco lightweight access point static IP address. The access point uses DHCP to get the IP address.
<i>Cisco_AP</i>		Cisco lightweight access point name.
<i>AP_IP_addr</i>		Cisco lightweight access point IP address
<i>IP_netmask/prefix_length</i>		Cisco lightweight access point network mask.
<i>gateway</i>		IP address of the Cisco lightweight access point gateway.
add		Adds a domain or DNS server.
domain		Specifies the domain to which a specific access point or all access points belong.
all		Specifies all access points.
<i>domain_name</i>		Specifies a domain name.
nameserver		Specifies a DNS server so that a specific access point or all access points can discover the controller using DNS resolution.
<i>nameserver-ip</i>		DNS server IP address.
delete		Deletes a domain or DNS server.



Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

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 both IPv4 and IPv6 address formats.
Usage Guidelines	<p>An access point cannot discover the controller using Domain Name System (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs.</p> <p>After you enter the IPv6 address, Prefix-length and IPv6 gateway address, the CAPWAP tunnel will restart for access point. Changing the AP's IP address will cause the AP to disjoin. After the access point rejoins the controller, you can enter the domain and IPv6 DNS server information.</p> <p>This command supports both IPv4 and IPv6 address formats.</p> <p>The following example shows how to configure static IP address on an access point:</p> <pre>(Cisco Controller) >config ap static-ip enable AP2 209.165.200.225 255.255.255.0 209.165.200.254</pre> <p>The following example shows how to configure static IPv6 address on an access point:</p> <pre>(Cisco Controller) > config ap static-ip enable AP2 2001:DB8:0:1::1</pre>	
Related Commands	show ap config general	

config ap stats-timer

To set the time in seconds that the Cisco lightweight access point sends its DOT11 statistics to the Cisco wireless LAN controller, use the **config ap stats-timer** command.

config ap stats-timer *period cisco_ap*

Syntax Description	<i>period</i>	Time in seconds from 0 to 65535. A zero value disables the timer.
	<i>cisco_ap</i>	Cisco lightweight access point name.
Command Default	The default value is 0 (disabled state).	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	A value of 0 (zero) means that the Cisco lightweight access point does not send any DOT11 statistics. The acceptable range for the timer is from 0 to 65535 seconds, and the Cisco lightweight access point must be disabled to set this value.	

The following example shows how to set the stats timer to 600 seconds for access point AP2:

```
(Cisco Controller) > config ap stats-timer 600 AP2
```


config ap syslog host global

To configure a global syslog server for all access points that join the controller, use the **config ap syslog host global** command.

config ap syslog host global *ip_address*

Syntax Description	<i>ip_address</i>	IPv4/IPv6 address of the syslog server.
Command Default	The default value of the IPv4 address of the syslog server is 255.255.255.255.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

By default, the global syslog server IP address for all access points is 255.255.255.255. Make sure that the access points can reach the subnet on which the syslog server resides before configuring the syslog server on the controller. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure a global syslog server, using IPv4 address, for all access points:

```
(Cisco Controller) > config ap syslog host global 255.255.255.255
```

The following example shows how to configure a global syslog server, using IPv6 address, for all access points:

```
(Cisco Controller) > config ap syslog host global 2001:9:10:56::100
```

config ap syslog host specific

To configure a syslog server for a specific access point, use the **config ap syslog host specific** command.

config ap syslog host specific *ap_name**ip_address*

Syntax Description	<i>ap_name</i>	Cisco lightweight access point.
	<i>ip_address</i>	IPv4/IPv6 address of the syslog server.

Command Default	The default value of the syslog server IP address is 0.0.0.0.
-----------------	---

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines	By default, the syslog server IP address for each access point is 0.0.0.0, indicating that it is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.
------------------	---

This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure a syslog server:

```
(Cisco Controller) >config ap syslog host specific 0.0.0.0
```

The following example shows how to configure a syslog server for a specific AP, using IPv6 address:

```
(Cisco Controller) > config ap syslog host specific AP3600 2001:9:10:56::100
```

config ap tcp-mss-adjust

To enable or disable the TCP maximum segment size (MSS) on a particular access point or on all access points, use the **config ap tcp-mss-adjust** command.

config ap tcp-mss-adjust {enable | disable} {cisco_ap | all} size

Syntax Description	enable	Enables the TCP maximum segment size on an access point.
	disable	Disables the TCP maximum segment size on an access point.
	<i>cisco_ap</i>	Cisco access point name.
	all	Specifies all access points.
	<i>size</i>	Maximum segment size. <ul style="list-style-type: none"> IPv4—Specify a value between 536 and 1363. IPv6—Specify a value between 1220 and 1331. <p>Note Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP.</p>



Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

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 IPv6.

Usage Guidelines When you enable this feature, the access point checks for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

This example shows how to enable the TCP MSS on access point cisco_ap1 with a segment size of 1200 bytes:

```
(Cisco Controller) > config ap tcp-mss-adjust enable cisco_ap1 1200
```

config ap telnet

To enable Telnet connectivity on an access point, use the **config ap telnet** command.

config ap telnet { **enable** | **disable** | **default** } *cisco_ap* | *all*

Syntax Description

enable	Enables the Telnet connectivity on an access point.
disable	Disables the Telnet connectivity on an access point.
default	Replaces the specific Telnet configuration of an access point with the global Telnet configuration.
<i>cisco_ap</i>	Cisco access point name.
<i>all</i>	All 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

- The Cisco lightweight access point associates with this controller for all network operation and in the event of a hardware reset.
- Telnet is not supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs.

The following example shows how to enable Telnet connectivity on access point cisco_ap1:

```
(Cisco Controller) >config ap telnet enable cisco_ap1
```

The following example shows how to disable Telnet connectivity on access point cisco_ap1:

```
(Cisco Controller) > config ap telnet disable cisco_ap1
```

config ap tertiary-base

To set the Cisco lightweight access point tertiary controller, use the **config ap tertiary-base** command.

config ap tertiary-base *controller_name* *Cisco_AP* [*controller_ip_address*]

Syntax Description	<i>controller_name</i>	Name of the controller.
	<i>Cisco_AP</i>	Cisco lightweight access point name.
	<i>controller_ip_address</i>	(Optional) If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller.
	Note	For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.
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 both IPv4 and IPv6 address formats.
Usage Guidelines	OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.	
	The Cisco lightweight access point associates with this controller for all network operations and in the event of a hardware reset.	
	This command supports both IPv4 and IPv6 address formats.	
	This example shows how to set the access point tertiary controller:	
	<pre>(Cisco Controller) > config ap tertiary-base SW_1 AP02 10.0.0.0</pre>	
Related Commands	The following example shows how to set an access point tertiary controller IPv6 address for an Cisco AP:	
	<pre>(Cisco Controller) > config ap tertiary-base SW_1 AP2 2001:DB8:0:1::1</pre>	
	show ap config general	

config ap tftp-downgrade

To configure the settings used for downgrading a lightweight access point to an autonomous access point, use the **config ap ftp-downgrade** command.

config ap tftp-downgrade *tftp_ip_addressfilename Cisco_AP*

Syntax Description	<i>tftp_ip_address</i>	IP address of the TFTP server.
	<i>filename</i>	Filename of the access point image file on the TFTP server.
	<i>Cisco_AP</i>	Access point name.
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 both IPv4 and IPv6 address formats.

The following example shows how to configure the settings for downgrading access point ap1240_102301:

```
(Cisco Controller) >config ap ftp-downgrade 209.165.200.224 1238.tar ap1240_102301
```

config ap username

To assign a username and password to access either a specific access point or all access points, use the **config ap username** command.

config ap username *user_id* **password** *passwd* [**all** | *ap_name*]

Syntax Description	<i>user_id</i>	Administrator username.
	<i>passwd</i>	Administrator password.
	all	(Optional) Specifies all access points.
	<i>ap_name</i>	Name of a specific 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 example shows how to assign a username and password to a specific access point:

```
(Cisco Controller) > config ap username jack password blue 1a204
```

The following example shows how to assign the same username and password to a all access points:

```
(Cisco Controller) > config ap username jack password blue all
```

config ap venue

To configure the venue information for 802.11u network on an access point, use the **config ap venue** command.

config ap venue { **add**venue_name venue-group venue-type lang-code cisco-ap | **delete** }

Syntax Description	add	Adds venue information.
	<i>venue_name</i>	Venue name.
	<i>venue_group</i>	Venue group category. See the table below for details on venue group mappings.
	<i>venue_type</i>	Venue type. This value depends on the venue-group specified. See the table below for venue group mappings.
	<i>lang_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).
	<i>cisco_ap</i>	Name of the access point.
	deletes	Deletes venue information.
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 set the venue details for an access point named cisco-ap1:

```
(Cisco Controller) > config ap venue add test 11 34 eng cisco-ap1
```

This table lists the different venue types for each venue group.

Table 2: Venue Group Mapping

Venue Group Name	Value	Venue Type for Group
UNSPECIFIED	0	

Venue Group Name	Value	Venue Type for Group
ASSEMBLY	1	<ul style="list-style-type: none"> • 0—UNSPECIFIED ASSEMBLY • 1—ARENA • 2—STADIUM • 3—PASSENGER TERMINAL (E.G., AIRPORT, BUS, FERRY, TRAIN STATION) • 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
BUSINESS	2	<ul style="list-style-type: none"> • 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

Venue Group Name	Value	Venue Type for Group
EDUCATIONAL	3	<ul style="list-style-type: none"> • 0—UNSPECIFIED EDUCATIONAL • 1—SCHOOL, PRIMARY • 2—SCHOOL, SECONDARY • 3—UNIVERSITY OR COLLEGE
FACTORY-INDUSTRIAL	4	<ul style="list-style-type: none"> • 0—UNSPECIFIED FACTORY AND INDUSTRIAL • 1—FACTORY
INSTITUTIONAL	5	<ul style="list-style-type: none"> • 0—UNSPECIFIED INSTITUTIONAL • 1—HOSPITAL • 2—LONG-TERM CARE FACILITY (E.G., NURSING HOME, HOSPICE, ETC.) • 3—ALCOHOL AND DRUG RE-HABILITATION CENTER • 4—GROUP HOME • 5—PRISON OR JAIL
MERCANTILE	6	<ul style="list-style-type: none"> • 0—UNSPECIFIED MERCANTILE • 1—RETAIL STORE • 2—GROCERY MARKET • 3—AUTOMOTIVE SERVICE STATION • 4—SHOPPING MALL • 5—GAS STATION
RESIDENTIAL	7	<ul style="list-style-type: none"> • 0—UNSPECIFIED RESIDENTIAL • 1—PRIVATE RESIDENCE • 2—HOTEL OR MOTEL • 3—DORMITORY • 4—BOARDING HOUSE
STORAGE	8	UNSPECIFIED STORAGE

Venue Group Name	Value	Venue Type for Group
UTILITY-MISC	9	0—UNSPECIFIED UTILITY AND MISCELLANEOUS
VEHICULAR	10	<ul style="list-style-type: none"> • 0—UNSPECIFIED VEHICULAR • 1—AUTOMOBILE OR TRUCK • 2—AIRPLANE • 3—BUS • 4—FERRY • 5—SHIP OR BOAT • 6—TRAIN • 7—MOTOR BIKE
OUTDOOR	11	<ul style="list-style-type: none"> • 0—UNSPECIFIED OUTDOOR • 1—MUNI-MESH NETWORK • 2—CITY PARK • 3—REST AREA • 4—TRAFFIC CONTROL • 5—BUS STOP • 6—KIOSK

config ap wlan

To enable or disable wireless LAN override for a Cisco lightweight access point radio, use the **config ap wlan** command.

```
config ap wlan {enable | disable} {802.11a | 802.11b} wlan_id cisco_ap
```

Syntax Description	enable	Enables the wireless LAN override on an access point.
	disable	Disables the wireless LAN override on an access point.
	802.11a	Specifies the 802.11a network.
	802.11b	Specifies the 802.11b network.
	wlan_id	Cisco wireless LAN controller ID assigned to a wireless LAN.
	cisco_ap	Cisco lightweight access point 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 enable wireless LAN override on the AP03 802.11a radio:

```
(Cisco Controller) > config ap wlan 802.11a AP03
```

config atf 802.11

Configure Cisco Air Time Fairness at the network level, at an AP group level, or at an AP radio level by using the **config atf 802.11** command.

config atf 802.11 {**a** | **b**} {**mode** {**disable** | **monitor** | **enforce-policy**} { [*ap-group-name*] | [*ap-name*] }} | {**optimization** {**enable** | **disable**}}

Syntax Description		
a		Specifies the 802.11a network settings
b		Specifies the 802.11b/g network settings
mode		Configures the granularity of Cisco ATF enforcement
disable		Disables Cisco ATF
monitor		Configures Cisco ATF in monitor mode
enforce-policy		Configures Cisco ATF in enforcement mode
optimization		Configures airtime optimization
enable		Enables airtime optimization
disable		Disabled airtime optimization
Command History	Release	Modification
	8.1	This command was introduced

- To configure Cisco ATF in monitor mode on an 802.11a network, enter this command:

```
(Cisco Controller) >config atf 802.11a mode monitor
```

- To enable airtime optimization on an 802.11a network, enter this command:

```
(Cisco Controller) >config atf 802.11a optimization enable
```

config atf policy

To configure Cisco Air Time Fairness (ATF) policies, use the **config atf policy** command.

```
config atf policy {{create policy-id policy-name policy-weight} | {modify {weight policy-weight policy-name}  
| {client-sharing {enable | disable} policy-name}} | {delete policy-name}}
```

Syntax Description

create	Creates an air time policy
modify	Modifies an air time policy
delete	Deletes an air time policy
client-sharing { enable disable } <i>policy-name</i>	Enables or disables client fair sharing for the specified policy name
<i>policy-id</i>	Policy ID between 1 and 511
<i>policy-name</i>	Name of the Cisco ATF policy
<i>policy-weight</i>	Policy weight between 5 and 100

Command History

Release	Modification
8.1.122.0	This command was introduced
8.2	client-sharing { enable disable } option was added.

This example shows how to create a Cisco ATF policy:

```
(Cisco Controller) >config atf policy create 2 test-policy 70
```

config auth-list add

To create an authorized access point entry, use the **config auth-list add** command.

```
config auth-list add {mic | ssc} AP_MAC [AP_key]
```

Syntax Description	mic	Specifies that the access point has a manufacture-installed certificate.
	ssc	Specifies that the access point has a self-signed certificate.
	AP_MAC	MAC address of a Cisco lightweight access point.
	AP_key	(Optional) Key hash value that is equal to 20 bytes or 40 digits.
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 create an authorized access point entry with a manufacturer-installed certificate on MAC address 00:0b:85:02:0d:20:

```
(Cisco Controller) > config auth-list add 00:0b:85:02:0d:20
```

- Related Commands
- config auth-list delete
 - config auth-list ap-policy

config auth-list ap-policy

To configure an access point authorization policy, use the **config auth-list ap-policy** command.

```
config auth-list ap-policy {authorize-ap {enable | disable} | ssc {enable | disable}}
```

Syntax Description	authorize-ap enable	Enables the authorization policy.
	authorize-ap disable	Disables the AP authorization policy.
	ssc enable	Allows the APs with self-signed certificates to connect.
	ssc disable	Disallows the APs with self-signed certificates to connect.
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 an access point authorization policy:

```
(Cisco Controller) > config auth-list ap-policy authorize-ap enable
```

The following example shows how to enable an access point with a self-signed certificate to connect:

```
(Cisco Controller) > config auth-list ap-policy ssc disable
```

Related Commands	config auth-list delete
	config auth-list add

config auth-list delete

To delete an access point entry, use the **config auth-list delete** command.

config auth-list delete *AP_MAC*

Syntax Description	<i>AP_MAC</i>	MAC address of a Cisco lightweight 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 example shows how to delete an access point entry for MAC address 00:1f:ca:cf:b6:60:

```
(Cisco Controller) > config auth-list delete 00:1f:ca:cf:b6:60
```

Related Commands	config auth-list delete
	config auth-list add
	config auth-list ap-policy

config avc profile create

To create a new Application Visibility and Control (AVC) profile, use the **config avc profile create** command.

config avc profile *profile_name* **create**

Syntax Description	<i>profile_name</i>	Name of the AVC profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
	create	Creates a new AVC profile.

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

Command History	Release	Modification
	7.4	This command was introduced.

Usage Guidelines

You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs. 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.

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

```
(Cisco Controller) > config avc profile avcprofile1 create
```

Related Commands	config avc profile delete config avc profile rule config wlan avc show avc profile show avc applications show avc statistics debug avc error debug avc events
-------------------------	--

config avc profile delete

To delete an Application Visibility and Control (AVC) profile, use the **config avc profile delete** command.

config avc profile *profile_name* **delete**

Syntax Description		
	<i>profile_name</i>	Name of the AVC profile.
	delete	Deletes an AVC profile.

Command Default The AVC profile is not deleted.

Command History	Release	Modification
	7.4	This command was introduced.

The following example shows how to delete an AVC profile:

```
(Cisco Controller) > config avc profile avcprofile1 delete
```

Related Commands	config avc profile create
	config avc profile rule
	config wlan avc
	show avc profile summary
	show avc profile detailed
	debug avc error
	debug avc events

config avc profile rule

To configure a rule for an Application Visibility and Control (AVC) profile, use the **config avc profile rule** command.

config avc profile *profile_name* **rule** {**add** | **remove**} **application** *application_name* {**drop** | **mark** *dscp*}

Syntax Description

<i>profile_name</i>	Name of the AVC profile.
rule	Configures a rule for the AVC profile.
add	Creates a rule for the AVC profile.
remove	Deletes a rule for the AVC profile.
application	Specifies the application that has to be dropped or marked.
<i>application_name</i>	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
drop	Drops the upstream and downstream packets that correspond to the chosen application.
mark	Marks the upstream and downstream packets that correspond to the chosen application with the Differentiated Services Code Point (DSCP) value that you specify in the drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.
<i>dscp</i>	Packet header code that is used to define the QoS across the Internet. The range is from 0 to 63.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to configure a rule for an AVC profile:

```
(Cisco Controller) > config avc profile avcprofile1 rule add application gmail mark 10
```

Related Commands

config avc profile delete
config avc profile create
config wlan avc
show avc profile
show avc applications
show avc statistics

debug avc error

debug avc events

config band-select cycle-count

To set the band select probe cycle count, use the **config band-select cycle-count** command.

config band-select cycle-count *count*

Syntax Description	<i>count</i>	Value for the cycle count between 1 to 10.
---------------------------	--------------	--

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 set the probe cycle count for band select to 8:

```
(Cisco Controller) > config band-select cycle-count 8
```

Related Commands	config band-select cycle-threshold
	config band-select expire
	config band-select client-rssi

config band-select cycle-threshold

To set the time threshold for a new scanning cycle, use the **config band-select cycle-threshold** command.

config band-select cycle-threshold *threshold*

Syntax Description	<i>threshold</i>	Value for the cycle threshold between 1 and 1000 milliseconds.				
Command Default	None					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>7.6</td><td>This command was introduced in a release earlier than Release 7.6.</td></tr></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 set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
(Cisco Controller) > config band-select cycle-threshold 700
```

Related Commands	config band-select cycle-count config band-select expire config band-select client-rssi
------------------	--

config band-select expire

To set the entry expire for band select, use the **config band-select expire** command.

config band-select expire { **suppression** | **dual-band** } *seconds*

Syntax Description	suppression	Sets the suppression expire to the band select.
	dual-band	Sets the dual band expire to the band select.
	<i>seconds</i>	<ul style="list-style-type: none"> • Value for suppression between 10 to 200 seconds. • Value for a dual-band between 10 to 300 seconds.

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 set the suppression expire to 70 seconds:

```
(Cisco Controller) > config band-select expire suppression 70
```

Related Commands	config band-select cycle-threshold
	config band-select client-rssi
	config band-select cycle-count

config band-select client-rssi

To set the client received signal strength indicator (RSSI) threshold for band select, use the **config band-select client-rssi** command.

config band-select client-rssi *rss*

Syntax Description	<i>rss</i> Minimum dBm of a client RSSI to respond to probe					
Command Default	None					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>7.6</td><td>This command was introduced in a release earlier than Release 7.6.</td></tr></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 set the RSSI threshold for band select to 70:

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

Related Commands	config band-select cycle-threshold config band-select expire config band-select cycle-count
-------------------------	--

config boot

To change a Cisco wireless LAN controller boot option, use the **config boot** command.

config boot { **primary** | **backup** }

Syntax Description

primary	Sets the primary image as active.
backup	Sets the backup image as active.

Command Default

The default boot option is **primary**.

Command History

Release	Modification
---------	--------------

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

Usage Guidelines

Each Cisco wireless LAN controller can boot off the primary, last-loaded operating system image (OS) or boot off the backup, earlier-loaded OS image.

The following example shows how to set the primary image as active so that the LAN controller can boot off the primary, last loaded image:

```
(Cisco Controller) > config boot primary
```

The following example shows how to set the backup image as active so that the LAN controller can boot off the backup, earlier loaded OS image:

```
(Cisco Controller) > config boot backup
```

Related Commands

show boot

config call-home contact email address

To configure the call-home contact email address, use the **config call-home contact-email-addr** command.

config call-home contact-email-addr *email-address*

Syntax Description	<i>email-address</i>		call-home contact email address
Command History	Release	Modification	
	8.2	This command was introduced.	

The following example shows how to add call-home contact email address:

```
(Cisco Controller) >config call-home contact-email-addr device1@example1.com
```

config call-home events

To enable or disable the call-home event reporting, use the **call-home events** command.

config call-home events { **enable** | **disable** }

Syntax Description
enable
disable

Command Default
Enable

Command History
Release
Modification
8.2

The following example shows how to disable call-home event reporting:

```
(Cisco Controller) > config call-home events disable
```

config call-home http-proxy ipaddr

To configure the http proxy address for reporting, use the **config call-home http-proxy ipaddr** command.

config call-home http-proxy ipaddr *ip-address* **port** *port*

Syntax Description	<i>ip-address</i>	the http-proxy IP address
	<i>port</i>	the http-proxy port number
Command History	Release Modification	
	8.2	This command was introduced.

The following example shows how to configure call home with the http-proxy IP address:

```
(Cisco Controller) >config call-home http-proxy ipaddr 209.165.200.224 port 773
```

config call-home http-proxy ipaddr 0.0.0.0

To reset the http proxy settings for reporting, use the **config call-home http-proxy ipaddr 0.0.0.0** command.

config call-home http-proxy ipaddr 0.0.0.0

Syntax Description	0.0.0.0	resets the http-proxy settings
--------------------	---------	--------------------------------

Command History	Release	Modification
	8.2	This command was introduced.

The following example shows how to reset call home http-proxy settings:

(Cisco Controller) >**config call-home http-proxy ipaddr 0.0.0.0**

config call-home profile

To create, update the call-home profile, use the **config call-home profile** command.

```
config call-home profile {create | update } profile-name {sm-license-data | all |
call-home-data } {short-text | long-text | xml } url
```

Syntax Description		
	create	create a Call-Home profile
	update	updates a Call-Home profile
	sm-license-data	Configures Smart license reporting profile
	all	Configures reporting profile for all modules
	call-home-data	Configures call home data reporting profile
	short-text	Configures data reporting in short-text format
	long-text	Configures data reporting in long-text format
	xml	Configures data reporting in XML format
	<i>url</i>	url name

Command History	Release	Modification
	8.2	This command was introduced.

The following example shows how to create a xml format reporting Call-Home profile:

```
(Cisco Controller) > config call-home profile create example-profile sm-license-data xml
internal.example.com
```

config call-home profile delete

To delete the call-home profile, use the **config call-home profile delete** command.

config call-home profile delete *profile-name*

Syntax Description	<i>profile-name</i>		Call-Home profile to be deleted.
Command History			
	Release	Modification	
	8.2	This command was introduced.	

The following example shows how to delete a Call-Home profile:

```
(Cisco Controller) > config call-home profile delete example-profile
```


config call-home profile status

To enable or disable the user profile, use the **config call-home profile status** command.

config call-home profile status { **enable** | **disable** }

Syntax Description	enable	enables the status of call-home profile
	disable	disables the status of call-home profile
Command History	Release Modification	
	8.2	This command was introduced.

The following example shows how to disable a Call-Home profile:

(Cisco Controller) >**config call-home profile status disable**

config call-home reporting

To set the privacy level for data reporting, use the **config call-home reporting data-privacy level** command.

config call-home reporting data-privacy level { **normal** | **high** } **hostname** *host name*

Syntax Description	normal	scrubs all normal-level commands
	high	scrubs all normal-level commands, the IP domain name and
	hostname	scrubs all high-level commands plus the hostname command
Command History	Release	Modification
	8.2	This command was introduced.

The following example shows how to configure normal privacy level:

```
(Cisco Controller) >config call-home reporting data-privacy- level normal hostname
internal.example.com
```

config call-home tac-profile

To enable or disable the tac-profile, use the **config call-home tac-profile status** command.

```
config call-home tac-profile status {enable | disable}
```

Syntax Description	enable	enables call-home TAC profile.
	disable	disables call-home TAC profile.
Command Default	Enable	
Command History	Release	Modification
	8.2	This command was introduced.

The following example shows how to disable call home tac-profile:

```
(Cisco Controller) >config call-home tac-profile status disable
```

config cdp

To configure the Cisco Discovery Protocol (CDP) on the controller, use the **config cdp** command.

```
config cdp {enable | disable | advertise-v2 {enable | disable} | timerseconds | holdtime holdtime_interval}
```

Syntax Description	enable	Enables CDP on the controller.
	disable	Disables CDP on the controller.
	advertise-v2	Configures CDP version 2 advertisements.
	timer	Configures the interval at which CDP messages are to be generated.
	seconds	Time interval at which CDP messages are to be generated. The range is from 5 to 254 seconds.
	holdtime	Configures the amount of time to be advertised as the time-to-live value in generated CDP packets.
	holdtime_interval	Maximum hold timer value. The range is from 10 to 255 seconds.

Command Default

The default value for CDP timer is 60 seconds.

The default value for CDP holdtime is 180 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 configure the CDP maximum hold timer to 150 seconds:

```
(Cisco Controller) > config cdp timer 150
```

- Related Commands**
- config ap cdp
 - show cdp
 - show ap cdp

config certificate

To configure Secure Sockets Layer (SSL) certificates, use the **config certificate** command.

config certificate { **generate** { **csr-webadmin** | **csr-webauth** | **webadmin** | **webauth** }

Syntax Description	generate	Specifies authentication certificate generation settings.
	csr-webadmin	Generates a new web administration certificate signing request.
	csr-webauth	Generates a new web authentication signing request.
	webadmin	Generates a new web administration certificate.
	webauth	Generates a new web authentication certificate.
Command Default	None	
Usage Guidelines	<p>With all parameters in CSR aligned with RFC-5280, there are some restrictions as follows:</p> <ul style="list-style-type: none"> • <i>emailAddress</i> in CSR can only be 128 characters long. • If the CSR is generated using the CLI, the maximum number of characters (of all input combined for CSR) is limited to 500 including config certificate generate csr-*****. 	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.3	This command was enhanced with new keywords in Release 8.3.

The following example shows how to generate a new web administration SSL certificate:

```
(Cisco Controller) > config certificate generate webadmin
Creating a certificate may take some time. Do you wish to continue? (y/n)
```

config certificate lsc

To configure Locally Significant Certificate (LSC) certificates, use the **config certificate lsc** command.

```
config certificate lsc {enable | disable | ca-server http://url:port/path | ca-cert {add | delete}
| subject-params country state city orgn dept email | other-params keysize} | ap-provision {auth-list
{add | delete} ap_mac | revert-cert retries}
```

Syntax Description

enable	Enables LSC certificates on the controller.
disable	Disables LSC certificates on the controller.
ca-server	Specifies the Certificate Authority (CA) server settings.
<i>http://url:port/path</i>	Domain name or IP address of the CA server.
ca-cert	Specifies CA certificate database settings.
add	Obtains a CA certificate from the CA server and adds it to the controller's certificate database.
delete	Deletes a CA certificate from the controller's certificate database.
subject-params	Specifies the device certificate settings.
<i>country state city orgn dept email</i>	Country, state, city, organization, department, and email of the certificate authority.
	Note The common name (CN) is generated automatically on the access point using the current MIC/SSC format <i>Cxxxx-MacAddr</i> , where <i>xxxx</i> is the product number.
other-params	Specifies the device certificate key size settings.
<i>keysize</i>	Value from 384 to 2048 (in bits); the default value is 2048.
ap-provision	Specifies the access point provision list settings.
auth-list	Specifies the provision list authorization settings.
<i>ap_mac</i>	MAC address of access point to be added or deleted from the provision list.
revert-cert	Specifies the number of times the access point attempts to join the controller using an LSC before reverting to the default certificate.
<i>retries</i>	Value from 0 to 255; the default value is 3.
	Note If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate. If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Command Default

The default value of *keysize* is 2048 bits. The default value of *retries* is 3.

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 CA server. To configure a different CA server, delete the configured CA server by using the **config certificate lsc ca-server delete** command, and then configure a different CA server.

If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in Step 8). If you do not configure an access point provision list, all access points with an MIC or SSC certificate that join the controller are LSC provisioned.

The following example shows how to enable the LSC settings:

```
(Cisco Controller) >config certificate lsc enable
```

This example shows how to enable the LSC settings for Certificate Authority (CA) server settings:

```
(Cisco Controller) >config certificate lsc ca-server http://10.0.0.1:8080/caserver
```

The following example shows how to add a CA certificate from the CA server and add it to the controller's certificate database:

```
(Cisco Controller) >config certificate lsc ca-cert add
```

The following example shows how to configure an LSC certificate with the keysize of 2048 bits:

```
(Cisco Controller) >config certificate lsc keysize 2048
```

config certificate ssc

To configure Self Signed Certificates (SSC) certificates, use the **config certificate ssc** command.

config certificate ssc hash validation { enable | disable }

Syntax Description

hash	Configures the SSC hash key.
validation	Configures hash validation of the SSC certificate.
enable	Enables hash validation of the SSC certificate.
disable	Disables hash validation of the SSC certificate.

Command Default

The SSC certificate is enabled by default..

Command History

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

Usage Guidelines

When you enable the SSC hash validation, an AP validates the SSC certificate of the virtual controller. When an AP validates the SSC certificate, it checks if the hash key of the virtual controller matches the hash key stored in its flash. If a match is found, the validation passes and the AP moves to the Run state. If a match is not found, the validation fails and the AP disconnects from the controller and restarts the discovery process. By default, hash validation is enabled. Hence, an AP must have the virtual controller hash key in its flash before associating with the virtual controller. If you disable hash validation of the SSC certificate, the AP bypasses the hash validation and directly moves to the Run state.

APs can associate with a physical controller, download the hash keys and then associate with a virtual controller. If the AP is associated to a physical controller and if hash validation is disabled, it joins any virtual controller without hash validation.

The following example shows how to enable hash validation of the SSC certificate:

```
(Cisco Controller) > config certificate ssc hash validation enable
```

Related Commands

show certificate ssc
show mobility group member
config mobility group member hash
config certificate
show certificate compatibility
show certificate lsc
show certificate summary
show local-auth certificates

config certificate use-device-certificate webadmin

To use a device certificate for web administration, use the **config certificate use-device-certificate webadmin** command.

config certificate use-device-certificate webadmin

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 use a device certificate for web administration:

```
(Cisco Controller) > config certificate use-device-certificate webadmin
Use device certificate for web administration. Do you wish to continue? (y/n) y
Using device certificate for web administration.
Save configuration and restart controller to use new certificate.
```

Related Commands	config certificate show certificate compatibility show certificate lsc show certificate ssc show certificate summary show local-auth certificates
-------------------------	--

config client ccx clear-reports

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

config client ccx clear-reports *client_mac_address*

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

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

Syntax Description	<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.
Usage Guidelines	<p>This test does not require the client to use the diagnostic channel.</p> <p>The following example shows how to send a request to the client00:0b:85:02:0d:20 to perform the default gateway ping test:</p> <pre>(Cisco Controller) >config client ccx default-gw-ping 00:0b:85:02:0d:20</pre>	

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*

Syntax Description	<i>client_mac_address</i> MAC address of the client.				
Command Default	None				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>7.6</td><td>This command was introduced in a release earlier than Release 7.6.</td></tr> </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.				
Usage Guidelines	<p>This test does not require the client to use the diagnostic channel.</p> <p>The following example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the DHCP test:</p> <pre>(Cisco Controller) >config client ccx dhcp-test 00:E0:77:31:A3:55</pre>				

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*

Syntax Description	<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.
Usage Guidelines	<p>This test does not require the client to use the diagnostic channel.</p> <p>The following example shows how to send a request to a client to perform the DNS server IP address ping test:</p> <pre>(Cisco Controller) >config client ccx dns-ping 00:E0:77:31:A3:55</pre>	

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*

Syntax Description	<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 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*

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

Syntax Description	<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 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*

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

- | | |
|-----------------------------|---|
| <i>message_type (cont.)</i> | <ul style="list-style-type: none"> • 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.
	dot11	(Optional) Specifies dot11 counters.
	security	(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*

Syntax Description	<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.
Usage Guidelines	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

client_mac_address MAC address of the client.

ssid Network name.

bssid Basic SSID.

802.11a Specifies the 802.11a network.

802.11b Specifies the 802.11b network.

802.11g Specifies the 802.11g network.

channel 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.
	802.11a	Specifies the 802.11a network.
	802.11b	Specifies the 802.11b network.
	802.11g	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.
	Note	The <i>profile_id</i> should be from one of the client profiles for which client reporting is enabled.
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 client location-calibration

To configure link aggregation, use the **config client location-calibration** command.

config client location-calibration { **enable** *mac_address interval* | **disable** *mac_address* }

Syntax Description	enable	(Optional) Specifies that client location calibration is enabled.
	<i>mac_address</i>	MAC address of the client.
	<i>interval</i>	Measurement interval in seconds.
	disable	(Optional) Specifies that client location calibration is disabled.
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 client location calibration for the client 37:15:85:2a with a measurement interval of 45 seconds:

```
(Cisco Controller) >config client location-calibration enable 37:15:86:2a:Bc:cf 45
```


config client profiling delete

To delete client profile , use the **config client profiling** command.

```
config client profiling delete { mac_address }
```

Syntax Description	mac_address	MAC address of the client.
Command History	Release	Modification
	8.2	This command was introduced in this release.

The following example shows how to delete a client profile:

```
(Cisco Controller) >config client profiling delete 37:15:86:2a:Bc:cf
```



Note Executing the above command changes the Device Type to "Unknown". The Client does not get deleted but instead the profiling info of the client is removed, and retains the client as it is still associated. There is no confirmation message from the CLI, due to architecture limitation of the controller.

config cloud-services cmx

To enable or disable CMX Cloud Services, use the **config cloud-services cmx** command.

config cloud-services cmx { **enable** | **disable** }

Syntax Description	enable	Enables the CMX Cloud Services
	disable	Disables the CMX Cloud Services
Command Default	None	
Command History	Release	Modification
	8.3	This command was introduced.

This example shows how to enable the CMX Cloud Services:

(Cisco Controller) > **config cloud-services cmx enable**

config cloud-services server url

To configure the Cloud Server URL, use the **config cloud-services server url** command.

config cloud-services server url *url*

Syntax Description	<i>url</i>	Enter the Cloud Server URL.
Command Default	None	
Command History	Release	Modification
	8.3	This command was introduced.

This example shows how to configure the Cloud Server URL:

```
(Cisco Controller) >config cloud-services server url www.example.com
```

config cloud-services server id-token

To configure the Cloud Server Id-Token, use the **config cloud-services server id-token** command.

config cloud-services server id-token *id-token*

Syntax Description	<i>id-token</i>	Enter the cloud server id-token.
Command Default	None	
Command History	Release	Modification
	8.3	This command was introduced.

This example shows how to configure the Cloud Server Id-Token:

(Cisco Controller) >**config cloud-services server id-token dzypisQ2#bo\$IAQM**

config coredump

To enable or disable the controller to generate a core dump file following a crash, use the **config coredump** command.

config coredump { **enable** | **disable** }

Syntax Description	enable	Enables the controller to generate a core dump file.
	disable	Disables the controller to generate a core dump file.
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 controller to generate a core dump file following a crash:

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

Related Commands	config coredump ftp
	config coredump username
	show coredump summary

config coredump ftp

To automatically upload a controller core dump file to an FTP server after experiencing a crash, use the **config coredump ftp** command.

config coredump ftp *server_ip_address filename*

Syntax Description	<i>server_ip_address</i>	IP address of the FTP server to which the controller sends its core dump file.
	<i>filename</i>	Name given to the controller core dump file.

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	The controller must be able to reach the FTP server to use this command.
------------------	--

The following example shows how to configure the controller to upload a core dump file named *core_dump_controller* to an FTP server at network address *192.168.0.13*:

```
(Cisco Controller) > config coredump ftp 192.168.0.13 core_dump_controller
```

Related Commands	config coredump
	config coredump username
	show coredump summary

config coredump username

To specify the FTP server username and password when uploading a controller core dump file after experiencing a crash, use the **config coredump username** command.

config coredump username *ftp_username* **password** *ftp_password*

Syntax Description	<i>ftp_username</i>	FTP server login username.
	<i>ftp_password</i>	FTP server login password.
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 must be able to reach the FTP server to use this command.	
	The following example shows how to specify a FTP server username of <i>admin</i> and password <i>adminpassword</i> for the core dump file upload:	
Related Commands	(Cisco Controller) > config coredump username admin password adminpassword	
	config coredump ftp	
	config coredump	
	show coredump summary	

config country

To configure the controller’s country code, use the **config country** command.

config country *country_code*

Syntax Description	<i>country_code</i> Two-letter or three-letter country code.	
Command Default	<i>us</i> (country code of the United States of America).	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	Controllers must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password-protected by the installer to maintain compliance with regulatory requirements and ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.	

You can use the **show country** command to display a list of supported countries.

The following example shows how to configure the controller’s country code to DE:

(Cisco Controller) >**config country DE**

config cts

To enable or disable Cisco TrustSec on controller, use the **config cts** command.

config cts {**enable** | **disable**}

Syntax Description	enable	Enables Cisco TrustSec on the controller
	disable	Disables Cisco TrustSec on the controller
Command Default	By default, Cisco TrustSec is in disabled state.	
Command History	Release	Modification
	8.4	This command was introduced.

config cts ap

To configure inline tagging and security group access control list (SGACL) enforcement on APs, use the **config cts ap** command.

config cts ap { **inline-tagging** | **sgacl-enforcement** } { **enable** | **disable** } { *ap-name* | **all** }

Syntax Description	inline-tagging	Configures inline tagging on all the APs or a specific AP
	sgacl-enforcement	Configures SGACL enforcement on all the APs or a specific AP
	enable	Enables the specified feature
	disable	Disables the specified feature
	<i>ap-name</i>	Name of the AP for which the specified feature has to be configured
	all	Configures the specified feature for all APs associated with the controller.

Command Default	By default, both inline tagging and SGACL enforcement are in disabled state.
-----------------	--

Command History	Release	Modification
	8.4	This command was introduced.

- | | |
|------------------|---|
| Usage Guidelines | <ul style="list-style-type: none">• Inline tagging is supported only on the APs in FlexConnect mode.• Inline tagging is not supported on Flex+Bridge 802.11ac lightweight APs.• Inline tagging and SGACL download or enforcement are not supported on these controllers: 5508, WiSM2, 8510, 7510, and vWLC.• If you enable SGACL enforcement for all the APs, the configuration is applied on all the APs except for the APs for which Cisco TrustSec override is enabled. |
|------------------|---|

The following example shows how to enable inline tagging on an AP named *cisco-flex-ap*:

```
(Cisco Controller) >config cts ap inline-tagging enable cisco-flex-ap
```

The following example shows how to enable SGACL enforcement on an AP named *cisco-flex-ap*:

```
(Cisco Controller) >config cts ap sgACL-enforcement enable cisco-flex-ap
```

config cts inline-tag

To configure Cisco TrustSec inline tagging for a controller, use the **config cts inline-tag** command.

```
config cts inline-tag {enable | disable}
```

Syntax Description	inline-tag Configures inline tagging for the controller	
	enable	Enables inline tagging
	disable	Disables inline tagging
Command Default	By default, inline tagging is in disabled state.	
Command History	Release	Modification
	8.4	This command was introduced.
Usage Guidelines	Inline tagging is not supported on these controllers: 5508, WiSM2, 8510, 7510, and vWLC.	

config cts ap override

To configure Cisco TrustSec override for an AP, use the **config cts ap override** command.

config cts ap override {**enable** | **disable**} {*ap-name*}

Syntax Description

enable	Enables CTS override for the corresponding AP
disable	Disables CTS override for the corresponding AP
<i>ap-name</i>	Name of the AP for which the CTS override has to be configured

Command Default

By default, CTS override for an AP is in disabled state.

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

If you enable SGACL enforcement for all the APs, the configuration is applied on all the APs except the APs for which CTS override is enabled.

The following example shows how to enable CTS override on an AP named *my-cisco-ap*:

```
(Cisco Controller) >config cts ap override enable my-cisco-ap
```

config cts device-id

To configure a Cisco TrustSec device ID, use the **config cts device-id** command.

config cts device-id *device-id* **password** *password*

Syntax Description	<i>device-id</i>	CTS device ID
	<i>password</i>	CTS device ID password
Command Default	None	
Command History	Release	Modification
	8.4	This command was introduced.

The following example shows how to configure a CTS device ID:

```
(Cisco Controller) > config cts device-id wlc-8540 password Cisco123
```

config cts refresh

To refresh Cisco TrustSec environment data or security group tag (SGT) policy, use the **config cts refresh** command.

config cts refresh { **environment-data** } | { **policy sgt** { **all** | *sgt-tag* } }

Syntax Description

environment-data	Refreshes CTS environment data
policy sgt	Refreshes SGT policy
all	Refreshes all SGT policies
<i>sgt-tag</i>	Enter the CTS SGT tag (an integer) to be refreshed

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

This example shows how to refresh the SGT policy, *Default-65535*:

```
(Cisco Controller) > config cts refresh policy sgt 65535
```

config cts sxp ap connection delete

To delete an SXPv4 connection peer for all the APs or a specific AP, use the **config cts sxp ap connection delete** command.

config cts sxp ap connection delete *ip-addr* { *cisco-ap* | **all** }

Syntax Description	<i>ip-addr</i>	SXPv4 IP address of a peer
	<i>cisco-ap</i>	Name of the AP.
	all	Applies the configuration to all the APs.
Command Default	None	
Command History	Release	Modification
	8.4	This command was introduced.

config cts sxp ap connection peer

To configure an SXPv4 peer connection for all the APs or a specific AP, use the **config cts sxp ap connection peer** command.

config cts sxp ap connection peer *ip-addr* **password** {**default** | **none**} **mode** {**both** | **listener** | **speaker**} {*cisco-ap* | **all**}

Syntax Description	<i>ip-addr</i>	SXPv4 IP address of the peer
	password	Configures password for the SXPv4 peer connection
	default	Uses default password for MD5 encryption
	none	Configures SXPv4 without password encryption
	<i>time-in-seconds</i>	Time after which an SXPv4 connection should be tried again after a failure to connect.
	mode	Configures mode of the SXPv4 connection
	both	Configures device as both SXP speaker and listener
	listener	Configures device as SXP listener
	speaker	Configures device as SXP speaker
	<i>cisco-ap</i>	Name of the AP
	all	Applies the configuration to all the APs associated with the corresponding controller
Command Default	None	
Command History	Release	Modification
	8.4	This command was introduced.

This example shows how to configure an SXPv4 peer connection with a default password and operate in both listener and speaker mode for all the APs associated with the controller:

```
(Cisco Controller) > config cts sxp ap connection peer 10.165.200.224 password default mode both all
```


config cts sxp ap default password

To configure the default password for an SXPv4 connection for all the APs or a specific AP, use the **config cts sxp ap default password** command.

```
config cts sxp ap default password password { cisco-ap | all }
```

Syntax Description	password	Default password for SXPv4 connection
	cisco-ap	Name of the AP
	all	Applies the configuration to all the APs associated with the corresponding controller
Command Default	None	
Command History	Release	Modification
	8.4	This command was introduced.

config cts sxp ap listener

To configure SXPv4 listener mode parameters, use the **config cts sxp ap listener** command.

config cts sxp ap listener hold-time *min-hold-time max-hold-time* { *cisco-ap* | **all** }

Syntax Description	<i>min-hold-time</i>	Minimum SXPv4 connection hold time
	<i>max-hold-time</i>	Maximum SXPv4 connection hold time
	<i>cisco-ap</i>	Name of the AP for which SXPv4 has to be configured
	all	Configures SXPv4 for all APs associated with the controller
Command Default	None	
Command History	Release	Modification
	8.4	This command was introduced.

config cts sxp ap reconciliation period

To configure SXPv4 connection reconciliation time period, use the **config cts sxp ap reconciliation period** command.

config cts sxp ap reconciliation period *time-in-seconds* { *cisco-ap* | **all** }

Syntax Description	<i>time-in-seconds</i>	Time interval until when the SXPv4 connection reconciles. Valid range is between 0 and 64000 seconds.
	<i>cisco-ap</i>	Name of the AP
	all	Applies the configuration to all the APs associated with the controller
Command Default	None	
Command History	Release	Modification
	8.4	This command was introduced.

config cts sxp ap retry period

To configure the interval between SXPv4 connection reattempts, use the **config cts sxp ap retry period** command.

config cts sxp ap retry period *time-in-seconds* { *cisco-ap* | **all** }

Syntax Description

<i>time-in-seconds</i>	Time after which an SXPv4 connection should be attempted again for after a failure to connect. Valid range is between 0 and 64000 seconds.
<i>cisco-ap</i>	Name of the AP
all	Applies the configuration to all the APs associated with the corresponding controller

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

config cts sxp ap speaker

To configure SXPv4 speaker mode parameters, use the **config cts sxp ap speaker** command.

config cts sxp ap speaker hold-time *time-in-seconds* { *cisco-ap* | **all** }

Syntax Description	<i>time-in-seconds</i>	Hold time interval, in seconds. Valid range is between 1 and 65534 seconds.
	<i>cisco-ap</i>	Name of the AP for which SXPv4 has to be configured
	all	Configures SXPv4 for all APs associated with the corresponding controller
Command Default	None	
Command History	Release	Modification
	8.4	This command was introduced.

config cts sxp

To enable or disable Cisco TrustSec SXP on a controller, use the **config cts sxp** command.

config cts sxp {enable | disable}

Syntax Description	enable	Enables Cisco TrustSec SXP on the controller
	disable	Disables Cisco TrustSec SXP on the controller
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

config cts sxp connection

To configure the CTS SXP connection on the controller, use the **config cts sxp connection** command.

config cts sxp connection { **delete** | **peer** } *ipv4-addr*

Syntax Description	delete	Deletes the SXP connection
	peer	Configures the next hop switch with which the controller is connected
	<i>ipv4-addr</i>	IPv4 address of the SXP connection
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

config cts sxp default password

To configure the default password for CTS SXP, use the **config cts sxp default password** command.

config cts sxp default password *password*

Syntax Description	<i>password</i> Default password for MD5 Authentication of SXP messages. The password should contain a minimum of six characters.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

config cts sxp retry period

To configure the interval between CTS SXP connection reattempts, use the **config cts sxp retry period** command.

config cts sxp retry period *time-in-seconds*

Syntax Description	<i>time-in-seconds</i> Time after which a CTS SXP connection should be attempted again for after a failure to connect. Valid range is between 0 and 64000 seconds.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

config cts sxp version

To configure the CTS SXP connection version, use the **config cts sxp version** command.

config cts sxp version *version-1-or-2*

Syntax Description	<i>version-1-or-2</i> Enter the SXP version. Valid values are 1 and 2				
Command Default	None				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>8.4</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	8.4	This command was introduced.
Release	Modification				
8.4	This command was introduced.				

config cts sxp

To configure Cisco TrustSec SXP (CTS) connections on the controller, use the **config cts sxp** command.

config cts sxp {**enable** | **disable** | **connection** {**delete** | **peer**} | **default password** *password* | **retry period** *time-in-seconds*}

Syntax Description		
enable		Enables CTS connections on the controller.
disable		Disables CTS connections on the controller.
connection		Configures CTS connection on the controller.
delete		Deletes the CTS connection on the controller.
peer		Configures the next hop switch with which the controller is connected.
<i>ip-address</i>		Only IPv4 address of the peer.
default password		Configures the default password for MD5 authentication of SXP messages.
<i>password</i>		Default password for MD5 Authentication of SXP messages. The password should contain a minimum of six characters.
retry period		Configures the SXP retry period.
<i>time-in-seconds</i>		Time after which a CTS connection should be again tried for after a failure to connect.

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

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

Usage Guidelines For release 8.0, only IPv4 is supported for TrustSec SXP configuration.

The following example shows how to enable CTS on the controller:

```
(Cisco Controller) > config cts sxp enable
```

The following example shows how to configure a peer for a CTS connection:

```
> config cts sxp connection peer 209.165.200.224
```

Related Commands	debug cts sxp
-------------------------	---------------

config custom-web ext-webauth-mode

To configure external URL web-based client authorization for the custom-web authentication page, use the **config custom-web ext-webauth-mode** command.

config custom-web ext-webauth-mode { **enable** | **disable** }

Syntax Description	enable	Enables the external URL web-based client authorization.
	disable	Disables the external URL we-based client authentication.
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 external URL web-based client authorization:

```
(Cisco Controller) > config custom-web ext-webauth-mode enable
```

Related Commands	config custom-web redirectUrl
	config custom-web weblogo
	config custom-web webmessage
	config custom-web webtitle
	config custom-web ext-webauth-url show custom-web

config custom-web ext-webauth-url

To configure the complete external web authentication URL for the custom-web authentication page, use the **config custom-web ext-webauth-url** command.

config custom-web ext-webauth-url *URL*

Syntax Description	<i>URL</i> URL used for web-based client authorization.				
Command Default	None				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>7.6</td><td>This command was introduced in a release earlier than Release 7.6.</td></tr> </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 complete external web authentication URL `http://www.AuthorizationURL.com/` for the web-based client authorization:

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

Related Commands	config custom-web redirectUrl config custom-web weblogo config custom-web webmessage config custom-web webtitle config custom-web ext-webauth-mode show custom-web
-------------------------	---

config custom-web ext-webserver

To configure an external web server, use the **config custom-web ext-webserver** command.

config custom-web ext-webserver { **add** *index IP_address* | **delete** *index* }

Syntax Description	add	Adds an external web server.
	<i>index</i>	Index of the external web server in the list of external web server. The index must be a number between 1 and 20.
	<i>IP_address</i>	IP address of the external web server.
	delete	Deletes 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.
	8.0	This command supports only IPv4 address format.

The following example shows how to add the index of the external web server 2 to the IP address of the external web server 192.23.32.19:

```
(Cisco Controller) > config custom-web ext-webserver add 2 192.23.32.19
```

Related Commands	config custom-web redirectUrl
	config custom-web weblogo
	config custom-web webmessage
	config custom-web webtitle
	config custom-web ext-webauth-mode
	config custom-web ext-webauth-url
	show custom-web

config custom-web logout-popup

To enable or disable the custom web authentication logout popup, use the **config custom-web logout-popup** command.

config custom-web logout-popup { enable | disable }

Syntax Description	enable	Enables the custom web authentication logout popup. This page appears after a successful login or a redirect of the custom web authentication page.
	disable	Disables the custom web authentication logout popup.
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 custom web authentication logout popup:

```
(Cisco Controller) > config custom-web logout-popup disable
```

Related Commands	config custom-web redirectUrl
	config custom-web weblogo
	config custom-web webmessage
	config custom-web webtitle
	config custom-web ext-webauth-url show custom-web

config custom-web qrscan-bypass-opt

To configure the qrscan bypass authentication options, use the **config custom-web qrscan-bypass-opt** command.

config custom-web qrscan-bypass-opt *timer count*

Syntax Description	<i>timer</i>	Set the duration to bypass the traffic temporarily. The range is between 5 and 60.
	<i>count</i>	Set the number of times the traffic can be bypassed before client rejoins. The range is between 1 and 9.
Command Default	None	
Command History	Release	Modification
	8.4	This command was introduced.

The following example shows how to set the custom qrscan bypass timer to 60 and number of times to 3 before the client rejoins:

```
(Cisco Controller) > config custom-web qrscan-bypass-opt 60 3
```


config custom-web radiusauth

To configure the RADIUS web authentication method, use the **config custom-web radiusauth** command.

config custom-web radiusauth {chap | md5chap | pap}

Syntax Description	chap	Configures the RADIUS web authentication method as Challenge Handshake Authentication Protocol (CHAP).
	md5chap	Configures the RADIUS web authentication method as Message Digest 5 CHAP (MD5-CHAP).
	pap	Configures the RADIUS web authentication method as Password Authentication Protocol (PAP).

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 RADIUS web authentication method as MD5-CHAP:

```
(Cisco Controller) > config custom-web radiusauth md5chap
```

Related Commands	config custom-web redirectUrl
	config custom-web webmessage
	config custom-web webtitle
	config custom-web ext-webauth-mode
	config custom-web ext-webauth-url
	show custom-web

config custom-web redirectUrl

To configure the redirect URL for the custom-web authentication page, use the **config custom-web redirectUrl** command.

config custom-web redirectUrl *URL*

Syntax Description*URL*

URL that is redirected to the specified address.

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 URL that is redirected to abc.com:

```
(Cisco Controller) > config custom-web redirectUrl abc.com
```

Related Commands**config custom-web weblogo****config custom-web webmessage****config custom-web webtitle****config custom-web ext-webauth-mode****config custom-web ext-webauth-url****show custom-web**

config custom-web sleep-client

To delete a web-authenticated sleeping client, use the **config custom-web sleep-client** command.

config custom-web sleep-client delete *mac_address*

Syntax Description	delete	Deletes a web-authenticated sleeping client with the help of the client MAC address.
	<i>mac_address</i>	MAC address of the sleeping client.
Command Default	The web-authenticated sleeping client is not deleted.	
Command History	Release	Modification
	7.5	This command was introduced.

The following example shows how to delete a web-authenticated sleeping client:

```
(Cisco Controller) > config custom-web sleep-client delete 0:18:74:c7:c0:90
```

config custom-web webauth-type

To configure the type of web authentication, use the **config custom-web webauth-type** command.

config custom-web webauth-type { **internal** | **customized** | **external** }

Syntax Description	internal	Configures the web authentication type to internal.
	customized	Configures the web authentication type to customized.
	external	Configures the web authentication type to external.

Command Default The default web authentication type is **internal**.

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 type of the web authentication type to internal:

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

- Related Commands
- config custom-web redirectUrl
 - config custom-web webmessage
 - config custom-web webtitle
 - config custom-web ext-webauth-mode
 - config custom-web ext-webauth-url
 - show custom-web

config custom-web weblogo

To configure the web authentication logo for the custom-web authentication page, use the **config custom-web weblogo** command.

config custom-web weblogo {enable | disable}

Syntax Description	enable	Enables the web authentication logo settings.
	disable	Enable or disable the web authentication logo 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 web authentication logo:

```
(Cisco Controller) > config custom-web weblogo enable
```

Related Commands	config custom-web redirectUrl
	config custom-web webmessage
	config custom-web webtitle
	config custom-web ext-webauth-mode
	config custom-web ext-webauth-url
	show custom-web

config custom-web webmessage

To configure the custom web authentication message text for the custom-web authentication page, use the **config custom-web webmessage** command.

config custom-web webmessage *message*

Syntax Description	<i>message</i>	Message text for web authentication.
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 message text Thisistheplace for webauthentication:

```
(Cisco Controller) > config custom-web webmessage Thisistheplace
```

Related Commands	config custom-web redirectUrl
	config custom-web weblogo
	config custom-web webtitle
	config custom-web ext-webauth-mode
	config custom-web ext-webauth-url
	show custom-web

config custom-web webtitle

To configure the web authentication title text for the custom-web authentication page, use the **config custom-web webtitle** command.

config custom-web webtitle *title*

Syntax Description	<i>title</i> Custom title text for web authentication.				
Command Default	None				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>7.6</td><td>This command was introduced in a release earlier than Release 7.6.</td></tr> </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 set the custom title text Helpdesk for web authentication:

```
(Cisco Controller) > config custom-web webtitle Helpdesk
```

Related Commands	config custom-web redirectUrl config custom-web weblogo config custom-web webmessage config custom-web ext-webauth-mode config custom-web ext-webauth-url show custom-web
------------------	--

config database size

To configure the local database, use the **config database size** command.

config database size *count*

Syntax Description	<i>count</i>	Database size value between 512 and 2040
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	Use the show database command to display local database configuration.	
	The following example shows how to configure the size of the local database:	
	(Cisco Controller) > config database size 1024	
Related Commands	show database	

config dhcp

To configure the internal DHCP, use the **config dhcp** command.

config dhcp { **address-pool** *scope start end* | **create-scope** *scope* | **default-router** *scope router_1* [*router_2*] [*router_3*] | **delete-scope** *scope* | **disable** *scope* | **dns-servers** *scope dns1* [*dns2*] [*dns3*] | **domain** *scope domain* | **enable** *scope* | **lease** *scope lease_duration* | **netbios-name-server** *scope wins1* [*wins2*] [*wins3*] | **network** *scope network netmask* }

config dhcpopt-82 remote-id { *ap_mac* | *ap_mac:ssid* | *ap-ethmac* | *apname:ssid* | *ap-group-name* | *flex-group-name* | *ap-location* | *apmac-vlan_id* | *apname-vlan_id* | *ap-ethmac-ssid* }

Syntax Description

address-pool <i>scope start end</i>	Configures an address range and specify the scope name and addresses of the address range.
create-scope <i>name</i>	Creates a new DHCP scope. <i>name</i> is the scope name.
default-router <i>scope router_1</i> [<i>router_2</i>] [<i>router_3</i>]	Configures the default routers and specify the IP address of the routers. You can specify the IP address of the primary, secondary, and tertiary routers.
delete-scope <i>scope</i>	Deletes the specified DHCP scope.
disable <i>scope</i>	Disables the specified DHCP scope.
dns-servers <i>scope dns1</i> [<i>dns2</i>] [<i>dns3</i>]	Configures the name servers for the scope. You must also specify at least one name server. Optionally, you can specify up to three name servers.
domain <i>scope domain</i>	Configures the DNS domain for the scope. Specify the scope and domain name.
enable <i>scope</i>	Enables the specified dhcp scope.
lease <i>scope lease_duration</i>	Configures the lease duration for the specified scope.
netbios-name-server <i>scope wins1</i> [<i>wins2</i>] [<i>wins3</i>]	Configures the netbios name servers for the scope. Specify the scope name and the IP address of the primary name server. Optionally, you can specify the IP address of secondary and tertiary name servers.
network <i>scope network netmask</i>	Configures the network and netmask for the scope. Specify the scope name, the IP address of the network, and the network mask.

opt-82 remote-id

Configures the DHCP option 82 format.

DHCP option 82 provides additional information. When DHCP is used to allocate network addresses, the controller acts as a DHCP relay agent. When a DHCP client requests from untrusted network, the controller adds option 82 information to the requests from clients before forwarding them to the DHCP server.

ap_mac

MAC address of the access point. This is the option 82 payload.

ap_mac:ssid

MAC address and SSID of the access point. This is the DHCP option 82 payload.

ap-ethmac

Remote ID format as AP Ethernet MAC address.

apname:ssid

Remote ID format as AP name and SSID.

ap-group-name

Remote ID format as AP group name.

flex-group-name

Remote ID format as FlexConnect group name.

ap-location

Remote ID format as AP location.

apmac-vlan_id

Remote ID format as AP radio MAC address:VLAN_ID.

apname-vlan_id

Remote ID format as AP Name:VLAN_ID.

ap-ethmac-ssid

Remote ID format as AP Ethernet MAC address and SSID.

Command Default

The default value for ap-group-name is default-group, and for ap-location, the default value is default location. If ap-group-name and flex-group-name are null, the system MAC is sent as the remote ID field.

Command History

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

Usage Guidelines

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

The following example shows how to configure the DHCP lease for the scope 003:

```
(Cisco Controller) >config dhcp lease 003
```

config dhcp opt-82 format

To configure the DHCP option 82 format, use the **config dhcp opt-82 format** command.

```
config dhcp opt-82 format { binary | ascii }
```

Syntax Description	<i>binary</i>	Specifies the DHCP option 82 format as binary.
	<i>ascii</i>	Specifies the DHCP option 82 format as ASCII.
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 format of DHCP option 82 payload:

```
(Cisco Controller) > config dhcp opt-82 format binary
```

config dhcp opt-82 remote-id

To configure the format of the DHCP option 82 payload, use the **config dhcp opt-82 remote-id** command.

config dhcp opt-82 remote-id {*ap_mac* | *ap_mac:ssid* | *ap-ethmac* | *apname:ssid* | *ap-group-name* | *flex-group-name* | *ap-location* | *apmac-vlan-id* | *apname-vlan-id* | *ap-ethmac-ssid*}

Syntax Description		
	<i>ap_mac</i>	Specifies the radio MAC address of the access point to the DHCP option 82 payload.
	<i>ap_mac:ssid</i>	Specifies the radio MAC address and SSID of the access point to the DHCP option 82 payload.
	<i>ap-ethmac</i>	Specifies the Ethernet MAC address of the access point to the DHCP option 82 payload.
	<i>apname:ssid</i>	Specifies the AP name and SSID of the access point to the DHCP option 82 payload.
	<i>ap-group-name</i>	Specifies the AP group name to the DHCP option 82 payload.
	<i>flex-group-name</i>	Specifies the FlexConnect group name to the DHCP option 82 payload.
	<i>ap-location</i>	Specifies the AP location to the DHCP option 82 payload.
	<i>apmac-vlan-id</i>	Specifies the radio MAC address of the access point and the VLAN ID to the DHCP option 82 payload.
	<i>apname-vlan-id</i>	Specifies the AP name and its VLAN ID to the DHCP option 82 payload.
	<i>ap-ethmac-ssid</i>	Specifies the Ethernet MAC address of the access point and the SSID to the DHCP option 82 payload.
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 remote ID of DHCP option 82 payload:

```
(Cisco Controller) > config dhcp opt-82 remote-id apgroup1
```

config dhcp proxy

To specify the level at which DHCP packets are modified, use the **config dhcp proxy** command.

```
config dhcp proxy {enable | disable {bootp-broadcast [enable | disable]}}
```

Syntax Description	enable	Allows the controller to modify the DHCP packets without a limit.
	disable	Reduces the DHCP packet modification to the level of a relay.
	bootp-broadcast	Configures DHCP BootP broadcast option.

Command Default	DHCP is enabled.
-----------------	------------------

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

Usage Guidelines

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

To enable third-party WGB support, you must enable the passive-client feature on the wireless LAN by entering the **config wlan passive-client enable** command.

The following example shows how to disable the DHCP packet modification:

```
(Cisco Controller) >config dhcp proxy disable
```

The following example shows how to enable the DHCP BootP broadcast option:

```
(Cisco Controller) >config dhcp proxy disable bootp-broadcast enable
```

config dhcp timeout

To configure a DHCP timeout value, use the **config dhcp timeout** command. If you have configured a WLAN to be in DHCP required state, this timer controls how long the controller will wait for a client to get a DHCP lease through DHCP.

config dhcp timeout *timeout-value*

Syntax Description	<i>timeout-value</i>	Timeout value in the range of 5 to 120 seconds.
Command Default	The default timeout value is 120 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 set the DHCP timeout to 10 seconds:

(Cisco Controller) >**config dhcp timeout 10**

config dx

To configure data externalization on a controller, use the **config dx** command.

config dx {**enable** | **disable**}

Syntax Description	enable	Enables data externalization on controller.
	disable	Disables data externalization on controller.
Command History	Release	Modification
	8.4	This command was introduced.
Usage Guidelines	If you have enabled data externalization on Cisco 5508 WLC, the maximum number of APs that the WLC can support is capped at 250.	

config exclusionlist

To create or delete an exclusion list entry, use the **config exclusionlist** command.

config exclusionlist {**add** *MAC* [*description*] | **delete** *MAC* | **description** *MAC* [*description*] }

Syntax Description	config exclusionlist	Configures the exclusion list.
	add	Creates a local exclusion-list entry.
	delete	Deletes a local exclusion-list entry
	description	Specifies the description for an exclusion-list entry.
	<i>MAC</i>	MAC address of the local Excluded entry.
	<i>description</i>	(Optional) Description, up to 32 characters, for an excluded entry.
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 create a local exclusion list entry for the MAC address *xx:xx:xx:xx:xx:xx*:

(Cisco Controller) > **config exclusionlist add *xx:xx:xx:xx:xx:xx* lab**

The following example shows how to delete a local exclusion list entry for the MAC address *xx:xx:xx:xx:xx:xx*:

(Cisco Controller) > **config exclusionlist delete *xx:xx:xx:xx:xx:xx* lab**

Related Commands **show exclusionlist**

config fabric

To enable or disable fabric, use the **config fabric** command.

config fabric enable disable

Syntax Description	enable	Enables fabric.
	disable	Disables fabric.
Command Default	None	
Command History	Release	Modification
	8.5	This command was introduced.

Example

The following example shows how to enable fabric:

```
config fabric enable
```

config fabric vnid create name

To configure the fabric Virtual Extensible LAN (VXLAN) network identifier (VNID) and subnet, use the **config fabric vnid create name** command.

config fabric vnid create name *interface-name* **l2-vnid** *l2-vnid* **ip** *network-ip* **subnet** *subnet* **l3-vnid** *l3-vnid*

Syntax Description	<i>interface-name</i>	Name of the interface.
	l2-vnid	Layer 2 VNID.
	<i>L2-vnid</i>	Layer 2 VNID value.
	ip	IP address.
	<i>network-ip</i>	Network IP address.
	subnet	Subnet address.
	<i>subnet</i>	Subnet address of the network.
	<i>L3-vnid</i>	Layer 3 VNID value.
	l3-vnid	Layer 3 VNID.

Command Default None

Command History	Release	Modification
	8.5	This command was introduced.

Usage Guidelines

The Subnet to VNID combination is expected to 1:1 with no-overlaps.

The VNID name can be used for Radius override or configuration of VNID on WLAN.

The guest fabric VNID or subnet should not overlap with the enterprise fabric VNID or subnet.

Examples

The following example shows how to configure fabric VNID and its subnet:

```
(Cisco Controller) >config fabric vnid create name vnid1 l2-vnid l2-vn ip 10.10.1.3 subnet 255.255.255.223 l3-vnid l3-vn
```

config fabric control-plane enterprise-fabric

To configure IP address of the mapserver and the pre-shared key, use the **config fabric control-plane enterprise-fabric ip** command.

config fabric control-plane enterprise-fabric {add |delete}{primary | secondary} ip *ip-address* preshared-key *pre-shared-key*

Syntax Description	<table> <tr> <td><i>ip-address</i></td><td>IP address of the mapserver.</td></tr> <tr> <td><i>pre-shared-key</i></td><td>Pre-shared key.</td></tr> </table>	<i>ip-address</i>	IP address of the mapserver.	<i>pre-shared-key</i>	Pre-shared key.
<i>ip-address</i>	IP address of the mapserver.				
<i>pre-shared-key</i>	Pre-shared key.				
Command Default	None				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>8.5</td><td>This command was introduced.</td></tr> </table>	Release	Modification	8.5	This command was introduced.
Release	Modification				
8.5	This command was introduced.				
Usage Guidelines	<p>The AP should be part of the fabric on the mapserver configured using this command. You can use a maximum of 2 IP addresses, which will be in active-active mode .</p> <p>Use config fabric control-plane enterprise-fabric delete ip<i>ip-address</i>command to delete the associated map server.</p>				
Examples	<p>The following example shows how to configure IP address of the mapserver and the pre-shared key:</p> <pre>(Cisco Controller) >config fabric control-plane enterprise-fabric add primary ip 10.1.1.1 preshare-key secret</pre>				

config fabric control-plane guest-fabric

To configure IP address of the guest mapserver and the pre-shared key used for the fabric WLAN, use the **config fabric control-plane guest-fabric** command.

config fabric control-plane guest-fabric {add |delete}{primary | secondary} ip *ip-address* preshared-key *pre-shared-key*

Syntax Description

ip-address IP address of the mapserver.

pre-shared-key Pre-shared key.

Command Default

Enterprise fabric mapserver is used.

Command History

Release	Modification
---------	--------------

8.5	This command was introduced.
-----	------------------------------

Usage Guidelines

You can use a maximum of 2 IP addresses, which will be in active-active mode .

Examples

The following example shows how to configure IP address of the guest mapserver and the pre-shared key:

```
(Cisco Controller) >config fabric control-plane guest-fabric add primary ip 10.2.1.1  
preshared-key guest
```

config flexconnect [ipv6] acl

To apply access control lists that are configured on a FlexConnect access point, use the **config flexconnect [ipv6] acl** command. Use the **ipv6** keyword to configure IPv6 FlexConnect ACLs .

config flexconnect [ipv6] acl {apply | create | delete} acl_name

Syntax Description	ipv6	Use this option to configure IPv6 FlexConnect ACLs. If you don't use this option, then IPv4 FlexConnect ACLs will be configured.
	apply	Applies an ACL to the data path.
	create	Creates an ACL.
	delete	Deletes an ACL.
	<i>acl_name</i>	ACL name that contains up to 32 alphanumeric characters.
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.8	IPv6 ACL option was introduced.

The following example shows how to apply the IPv4 ACL configured on a FlexConnect access point:

```
(Cisco Controller) >config flexconnect acl apply acl1
```

config flexconnect [ipv6] acl rule

To configure access control list (ACL) rules on a FlexConnect access point, use the **config flexconnect [ipv6] acl rule** command.

config flexconnect [ipv6] acl rule {**action** *rule_name rule_index* {**permit** | **deny**} | **add** *rule_name rule_index* | **change index** *rule_name old_index new_index* | **delete** *rule_name rule_index* | **destination address** *rule_name rule_index ip_address netmask* | **destination port range** *rule_name rule_index start_port end_port* | **direction** *rule_name rule_index* {**in** | **out** | **any**} | **dscp** *rule_name rule_index dscp* | **protocol** *rule_name rule_index protocol* | **source address** *rule_name rule_index ip_address netmask* | **source port range** *rule_name rule_index start_port end_port* | **swap index** *rule_name index_1 index_2*}

Syntax Description		
ipv6		Use this option to configure IPv6 FlexConnect ACL rules. If you don't use this option, then IPv4 FlexConnect ACL rules will be configured.
action		Configures whether to permit or deny access.
<i>rule_name</i>		ACL name that contains up to 32 alphanumeric characters.
<i>rule_index</i>		Rule index between 1 and 32.
permit		Permits the rule action.
deny		Denies the rule action.
add		Adds a new rule.
change		Changes a rule's index.
index		Specifies a rule index.
delete		Deletes a rule.
destination address		Configures a rule's destination IP address and netmask.
<i>ip_address</i>		IP address of the rule.
<i>netmask</i>		Netmask of the rule.
<i>start_port</i>		Start port number (between 0 and 65535).
<i>end_port</i>		End port number (between 0 and 65535).
direction		Configures a rule's direction to in, out, or any.
in		Configures a rule's direction to in.
out		Configures a rule's direction to out.
any		Configures a rule's direction to any.
dscp		Configures a rule's DSCP.

<i>dscp</i>	Number between 0 and 63, or any .
protocol	Configures a rule's DSCP.
<i>protocol</i>	Number between 0 and 255, or any .
source address	Configures a rule's source IP address and netmask.
source port range	Configures a rule's source port range.
swap	Swaps two rules' indices.
<i>index_1</i>	The rule first index to swap.
<i>index_2</i>	The rule index to swap the first index with.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.8	IPv6 ACL option was introduced.

This example shows how to configure an ACL to permit access:

```
(Cisco Controller) >config flexconnect acl rule action lab1 4 permit
```

config flexconnect [ipv6] acl url-domain

To configure a URL domain-based rule for a FlexConnect ACL, use the **config flexconnect acl [ipv6] url-domain** command.

config flexconnect [**ipv6**]**acl url-domain** {**action** *acl-name index action* | **add** *acl-name index* | **delete** *acl-name index* | **url** *acl-name index url-name*}

Syntax Description

ipv6	Use this option to configure URL domain-based rules for IPv6 FlexConnect ACLs. If you don't use this option, then IPv4 FlexConnect ACL rules will be configured.
action <i>acl-name index action</i>	Configures the action for the FlexConnect ACL rule, whether to permit or deny access.
add <i>acl-name index</i>	Adds URL domain to the FlexConnect ACL.
delete <i>acl-name index</i>	Deletes the URL domain from the FlexConnect ACL.
url <i>acl-name index url-name</i>	Configures the URL name in the FlexConnect ACL.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.8	IPv6 ACL option was introduced.

This example shows how to configure URL-based rule for an IPv6 FlexConnect ACL:

```
(Cisco Controller) >config flexconnect ipv6 acl url-domain action acls-to-allow 2 permit
```


config flexconnect arp-caching

To save an ARP entry for a client in the cache with locally switched WLAN on FlexConnect APs or in a software-defined access (Fabric) deployment, use **config flexconnect arp-caching** command.

config flexconnect arp-caching {enable } disable}

Syntax Description	arp-caching enable	Instructs the access point to save the ARP entry for a client in the cache and reply on its behalf of the client for locally switched WLAN.
	arp-caching disable	Disables ARP caching.
Command Default	None	
Command History	Release	Modification
	8.0	This command was introduced.
	8.5.151.0, 8.8.12x.0, 8.9.111.0, 8.10	This command was made applicable to software-defined access deployments as well.

Example

The following example shows how to apply the proxy ARP with locally switched WLAN on FlexConnect APs.

```
(Cisco Controller) >config flexconnect arp-caching enable
```

config flexconnect avc profile

To configure a Flexconnect Application Visibility and Control (AVC) profile, use the **config flexconnect avc profile** command.

config flexconnect avc profile *profilename* {**create** | **delete**} | **apply** | **rule** {**addapplication** *app-name* {**drop** | {**mark** *dscp-value*}} } | {**remove application** *app-name*}

Syntax Description

<i>proflie-name</i>	Name of the AVC profile. The range is from 0 to 32 alphanumeric characters.
create	Creates an AVC profile.
delete	Deletes an AVC profile.
apply	Applies an AVC profile.
rule	Configures a Rule for an AVC profile.
add application	Adds a rule for an AVC profile.
<i>app-name</i>	Name of the application. The range is from 0 to 32 alphanumeric characters.
drop	Adds a rule to drop packets.
mark	Adds a rule to mark packets with specific differentiated services code point (DSCP).
<i>dscp-value</i>	DSCP value for marking packets. The range is from 0 to 63.
remove application	Removes a rule for an AVC profile.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to create a FlexConnect profile:

```
(Cisco Controller) >config flexconnect avc profile profile1 create
```

config flexconnect fallback-radio-shut

To configure the radio interface of an access point when the Ethernet link is not operational, use the **config flexconnect fallback-radio-shut** command.

config flexconnect fallback-radio-shut { **disable** | **enable delay** *delay-in-sec* }

Syntax Description	disable	Disables the radio interface shutdown.
	enable	Enables the radio interface shutdown.
	delay	Specifies the delay for the interface after which the radio interface has to be shut down.
	<i>delay-in-sec</i>	Delay duration, in seconds.

Command Default	The radio interface shutdown is disabled.
------------------------	---

Command History	Release	Modification
	7.6	This command was introduced.

Usage Guidelines	You can specify the delay duration only if you enable the radio interface shutdown.
-------------------------	---

The following example shows how to enable the radio interface shutdown after a delay duration of 5 seconds:

```
(Cisco Controller) >config flexconnect fallback-radio-shut enable delay 5
```

config flexconnect group

To add, delete, or configure a FlexConnect group, use the **config flexconnect group** command.

```
config flexconnect group group_name {add | delete | ap {add | delete} ap-mac | radius {ap
{authority {id hex_id | info auth_info} | disable | eap-fast {enable | disable} | enable | leap
{enable | disable} | pac-timeout timeout | server-key {auto | key} | user {add {username
password} | delete username}}} | server auth {add | delete} {primary | secondary}
IP_address auth_port secret} | predownload {disable | enable} | master ap_name | slave
{retry-count max_count | ap-name cisco_ap} | start {primary backup abort} | local-split {wlan
wlan_id acl acl_name {enable | disable}} | multicast overridden-interface {enable | disable} |
vlan {add vlan_id acl in-aclname out-aclname | delete vlan_id} | web-auth wlan wlan_id acl acl_name
{enable | disable} | web-policy acl {add | delete} acl_name}
```

```
config flexconnect group group_name radius ap {eap-cert download | eap-tls {enable | disable}
| peap {enable | disable}}
```

```
config flexconnect group group_name policy acl {add | delete} acl_name
```

Syntax Description

<i>group_name</i>	Group name.
add	Adds a FlexConnect group.
delete	Deletes a FlexConnect group.
ap	Adds or deletes an access point.
add	Adds an access point to a FlexConnect group.
delete	Deletes an access point to a FlexConnect group.
<i>ap_mac</i>	MAC address of the access point.
radius	Configures the RADIUS server for the FlexConnect group.
ap	Configures an access point basic authentication for a FlexConnect group.
authority	Configures the Extensible Authentication via Secure Tunneling parameters.
id	Configures the authority identifier.
<i>hex_id</i>	Authority identifier of the local access point. You can enter up to 32 characters.
info	Configures the authority identifier in text format.

<i>auth_info</i>	Authority identifier of the
disable	Disables an AP based RADIUS
eap-fast	Enables or disables Extensible Authentication Protocol (EAP) Authentication via Secure
enable	Enables EAP-FAST authentication
disable	Disables EAP-FAST authentication
enable	Enables AP based RADIUS authentication
leap	Enables or disables Lightweight Extensible Authentication Protocol (LEAP) authentication.
disable	Disables LEAP authentication
enable	Enables LEAP authentication
pac-timeout	Configures the EAP-FAST Protected Access Credential (PAC) timeout parameters.
<i>timeout</i>	PAC timeout in days. The value 0 indicates that it is disabled.
server-key	Configures the EAP-FAST server key to encrypt and decrypt PACs.
auto	Automatically generates a key
<i>key</i>	Key that disables efficient
user	Manages the user list at the
add	Adds a user. You can configure
<i>username</i>	Username that is case-sensitive and 24 characters.
<i>password</i>	Password of the user.
delete	Deletes a user.
server	Configures an external RADIUS
add	Adds an external RADIUS
delete	Deletes an external RADIUS
primary	Configures an external primary
secondary	Configures an external secondary
<i>IP_address</i>	IP address of the RADIUS

<i>auth_port</i>	Port address of the RADIUS server.
<i>secret</i>	Index of the RADIUS server.
predownload	Configures an efficient AP upgrade. The AP can download an upgrade image without resetting the access point.
disable	Disables an efficient upgrade feature.
enable	Enables an efficient upgrade feature.
master	Manually designates an access point as the primary AP.
<i>ap_name</i>	Access point name.
slave	Manually designates an access point as a subordinate AP.
retry-count	Configures the number of times the AP can predownload an image from the server.
<i>max_count</i>	Maximum number of times the AP can predownload an image from the server.
ap_name	Override the manually configured access point name.
<i>cisco_ap</i>	Name of the primary access point.
start	Starts the predownload image.
primary	Starts the predownload primary group.
backup	Starts the predownload backup group.
abort	Terminates the predownload image group.
local-split	Configures a local-split ACL on the access point.
wlan	Configures a WLAN for a local split.
<i>wlan_id</i>	Wireless LAN identifier between the access point and the controller.
acl	Configures a local split ACL on the access point.
<i>acl_name</i>	Name of the ACL.
multicast overridden-interface	Configures multicast across the overridden interface for locally connected devices.
vlan	Configures a VLAN to the FlexConnect group.

add	Adds a VLAN to the FlexConnect group.
<i>vlan_id</i>	VLAN identifier.
<i>in-acl</i>	Inbound ACL name that controls access to the FlexConnect group.
<i>out-acl</i>	Outbound ACL name that controls access to the FlexConnect group.
delete	Deletes a VLAN from the FlexConnect group.
web-auth	Configures a FlexConnect group for web authentication.
wlan	Specifies the wireless LAN for the FlexConnect group.
<i>wlan_id</i>	Wireless LAN identifier for the FlexConnect group.
<i>cisco_ap</i>	Name of the FlexConnect group for Cisco APs.
acl	Configures a FlexConnect group for ACLs.
web-policy	Configures a web policy for the FlexConnect group.
add	Adds a web policy FlexConnect group.
delete	Deletes a web policy FlexConnect group.
eap-cert download	Downloads the EAP root certificate for the FlexConnect group.
eap-tls	Enables or disables EAP-TLS authentication for the FlexConnect group.
peap	Enables or disables Protected Extensible Authentication Protocol (PEAP) authentication for the FlexConnect group.
policy acl	Configures policy ACL for the FlexConnect group.
http-proxy ipaddress	Configures http-proxy server for the FlexConnect group.

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 add up to 100 clients.

Beginning in Release 7.4 and later releases, the supported maximum number of RADIUS servers is 100.

The following example shows how to add a FlexConnect group for MAC address 192.12.1.2:

```
(Cisco Controller) >config flexconnect group 192.12.1.2 add
```

The following example shows how to add a RADIUS server as a primary server for a FlexConnect group with the server index number 1:

```
(Cisco Controller) >config flexconnect group 192.12.1.2 radius server add primary 1
```

The following example shows how to enable a local split ACL on a FlexConnect AP group for a WLAN:

```
(Cisco Controller) >config flexconnect group flexgroup1 local-split wlan 1 acl flexacl1 enable
```


config flexconnect group vlan

To configure VLAN for a FlexConnect group, use the **config flexconnect group vlan** command.

```
config flexconnect group group_name vlan {add vlan-id acl in-aclname out-aclname | delete vlan-id}
```

Syntax Description	group_name	FlexConnect group name.
	add	Adds a VLAN for the FlexConnect group.
	vlan-id	VLAN ID.
	acl	Specifies an access control list.
	in-aclname	In-bound ACL name.
	out-aclname	Out-bound ACL name.
	delete	Deletes a VLAN from the FlexConnect group.
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 VLAN ID 1 for the FlexConnect group myflexacl where the in-bound ACL name is in-acl and the out-bound ACL is out-acl:

```
(Cisco Controller) >config flexconnect group vlan myflexacl vlan add 1 acl in-acl out-acl
```

config flexconnect group *group-name* dhcp overridden-interface

To enable or disable the DHCP overridden interface for a FlexConnect group, use the **config flexconnect group *group-name* dhcp overridden-interface** command.

```
config flexconnect group group-name dhcp overridden-interface {enable | disable}
```

Syntax Description	overridden-interface	The DHCP overridden interface for FlexConnect group.
	<i>group-name</i>	Name of the FlexConnect group.
	enable	Instructs the access point to enable DHCP broadcast for locally switched clients.
	disable	Disables the feature.
Command Default	None	
Command History	Release	Modification
	8.0	This command was introduced.

Example

The following example shows how to enable DHCP broadcast for locally switched clients.

```
(Cisco Controller) >config flexconnect
  group flexgroup dhcp overridden-interface enable
```

config flexconnect group web-auth

To configure Web-Auth ACL for a FlexConnect group, use the **config flexconnect group web-auth** command.

```
config flexconnect group group_name web-auth wlan wlan-id acl acl-name {enable | disable}
```

Syntax Description	<i>group_name</i>	FlexConnect group name.
	<i>wlan-id</i>	WLAN ID.
	<i>acl-name</i>	ACL name.
	enable	Enables the Web-Auth ACL for a FlexConnect group.
	disable	Disables the Web-Auth ACL for a FlexConnect group.

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-Auth ACL webauthacl for the FlexConnect group myflexacl on WLAN ID 1:

```
(Cisco Controller) >config flexconnect group myflexacl web-auth wlan 1 acl webauthacl enable
```

config flexconnect group web-policy

To configure Web Policy ACL for a FlexConnect group, use the **config flexconnect group web-policy** command.

config flexconnect group *group_name* **web-policy acl** {**add** | **delete**} *acl-name*

Syntax Description

<i>group_name</i>	FlexConnect group name.
add	Adds the Web Policy ACL.
delete	Deletes the Web Policy ACL.
<i>acl-name</i>	Name of the Web Policy ACL.

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 the Web Policy ACL mywebpolicyacl to the FlexConnect group myflexacl:

```
(Cisco Controller) >config flexconnect group myflexacl web-policy acl add mywebpolicyacl
```

config flexconnect join min-latency

To enable or disable the access point to choose the controller with the least latency when joining, use the **config flexconnect join min-latency** command.

config flexconnect join min-latency { **enable** | **disable** } *cisco_ap*

Syntax Description	enable	Enables the access point to choose the controller with the least latency when joining.
	disable	Disables the access point to choose the controller with the least latency when joining.
	<i>cisco_ap</i>	Cisco lightweight access point.

Command Default The access point cannot choose the controller with the least latency when joining.

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

Usage Guidelines When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the controller that responds first. This command is supported only on the following controller releases:

- Cisco 2500 Series Controller
- Cisco 5500 Series Controller
- Cisco Flex 7500 Series Controllers
- Cisco 8500 Series Controllers
- Cisco Wireless Services Module 2

This configuration overrides the HA setting on the controller, and is applicable only for OEAP access points.

The following example shows how to enable the access point to choose the controller with the least latency when joining:

```
(Cisco Controller) >config flexconnect join min-latency enable CISCO_AP
```

config flexconnect office-extend

To configure FlexConnect mode for an OfficeExtend access point, use the **config flexconnect office-extend** command.

config flexconnect office-extend [{enable | disable} *cisco_ap* | clear-personalssid-config *cisco_ap*]

Syntax Description

enable	Enables the OfficeExtend mode for an access point.
disable	Disables the OfficeExtend mode for an access point.
clear-personalssid-config	Clears only the access point's personal SSID.
<i>cisco_ap</i>	Cisco lightweight access point.

Command Default

OfficeExtend mode is enabled automatically when you enable FlexConnect mode on the access point.

Command History

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

Usage Guidelines

Currently, only Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 Series Controller with a WPlus license can be configured to operate as OfficeExtend access points.

Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. OfficeExtend access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. You can enable or disable rogue detection for a specific access point or for all access points by using the **config rogue detection** command.

DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point or for all access points by using the **config ap link-encryption** command.

Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point by using the **config ap telnet** or **config ap ssh** command.

Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point or for all access points currently associated to the controller by using the **config ap link-latency** command.

The following example shows how to enable the office-extend mode for the access point Cisco_ap:

```
(Cisco Controller) >config flexconnect office-extend enable Cisco_ap
```

The following example shows how to clear only the access point's personal SSID for the access point Cisco_ap:

```
(Cisco Controller) >config flexconnect office-extend clear-personalssid-config Cisco_ap
```

config flow

To configure a NetFlow Monitor and Exporter, use the **config flow** command.

```
config flow {add | delete} monitor monitor_name {exporter exporter_name |
record {ipv4_client_app_flow_record | ipv4_client_src_dst_flow_record}}
```

Syntax Description		
add		Associates either a NetFlow monitor with an exporter, or a NetFlow record with a NetFlow monitor.
delete		Dissociates either a NetFlow monitor from an exporter, or a NetFlow record from a NetFlow monitor.
monitor		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 in a monitor name.
exporter		Configures a NetFlow exporter.
<i>exporter_name</i>		Name of the NetFlow exporter. The exporter name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces in an exporter name.
record		Associates a NetFlow record to the NetFlow monitor.
<i>ipv4_client_app_flow_record</i>		Existing record template for better performance.
<i>ipv4_client_src_dst_flow_record</i>		Enhanced record template for better coverage.

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

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

Usage Guidelines

An exporter is a network entity that exports the template with IP traffic information. The controller acts as an exporter. A NetFlow record in the controller contains the information about the traffic in a given flow, such as client MAC address, client source IP address, WLAN ID, incoming and outgoing bytes of data, incoming and outgoing packets, and incoming and outgoing Differentiated Services Code Point (DSCP).

The following example shows how to configure a NetFlow monitor and exporter:

```
(Cisco Controller) > config flow add monitor monitor1 exporter exporter1
```

config guest-lan

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

config guest-lan {**create** | **delete**} *guest_lan_id* *interface_name* | {**enable** | **disable**} *guest_lan_id*

Syntax Description

create	Creates a wired LAN settings.
delete	Deletes a wired LAN settings.
<i>guest_lan_id</i>	LAN identifier between 1 and 5 (inclusive).
<i>interface_name</i>	Interface name up to 32 alphanumeric characters.
enable	Enables a wireless LAN.
disable	Disables a 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 enable a wireless LAN with the LAN ID 16:

```
(Cisco Controller) > config guest-lan enable 16
```

Related Commands

show wlan

config guest-lan custom-web ext-webauth-url

To redirect guest users to an external server before accessing the web login page, use the **config guest-lan custom-web ext-webauth-url** command.

config guest-lan custom-web ext-webauth-url *ext_web_url* *guest_lan_id*

Syntax Description	<i>ext_web_url</i>	URL for the external server.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
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 wireless LAN with the LAN ID 16:

```
(Cisco Controller) > config guest-lan custom-web ext-webauth-url
http://www.AuthorizationURL.com/ 1
```

Related Commands	config guest-lan
	config guest-lan create
	config guest-lan custom-web login_page

config guest-lan custom-web global disable

To use a guest-LAN specific custom web configuration rather than a global custom web configuration, use the **config guest-lan custom-web global disable** command.

config guest-lan custom-web global disable *guest_lan_id*

Syntax Description	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
---------------------------	---------------------	---

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 enter the config guest-lan custom-web global enable <i>guest_lan_id</i> command, the custom web authentication configuration at the global level is used.
-------------------------	---

The following example shows how to disable the global web configuration for guest LAN ID 1:

```
(Cisco Controller) > config guest-lan custom-web global disable 1
```

Related Commands	config guest-lan
	config guest-lan create
	config guest-lan custom-web ext-webauth-url
	config guest-lan custom-web login_page
	config guest-lan custom-web webauth-type

config guest-lan custom-web login_page

To enable wired guest users to log into a customized web login page, use the **config guest-lan custom-web login_page** command.

config guest-lan custom-web login_page *page_name* *guest_lan_id*

Syntax Description	<i>page_name</i>	Name of the customized web login page.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
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 customize a web login page custompage1 for guest LAN ID 1:

```
(Cisco Controller) > config guest-lan custom-web login_page custompage1 1
```

Related Commands	config guest-lan
	config guest-lan create
	config guest-lan custom-web ext-webauth-url

config guest-lan custom-web webauth-type

To define the web login page for wired guest users, use the **config guest-lan custom-web webauth-type** command.

config guest-lan custom-web webauth-type { **internal** | **customized** | **external** } *guest_lan_id*

Syntax Description	internal	Displays the default web login page for the controller. This is the default value.
	customized	Displays the custom web login page that was previously configured.
	external	Redirects users to the URL that was previously configured.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

Command Default	The default web login page for the controller is internal.
------------------------	--

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 guest LAN with the webauth-type as internal for guest LAN ID 1:

```
(Cisco Controller) > config guest-lan custom-web webauth-type internal 1
```

Related Commands	config guest-lan config guest-lan create config guest-lan custom-web ext-webauth-url
-------------------------	---

config guest-lan ingress-interface

To configure the wired guest VLAN's ingress interface that provides a path between the wired guest client and the controller through the Layer 2 access switch, use the **config guest-lan ingress-interface** command.

config guest-lan ingress-interface *guest_lan_id* *interface_name*

Syntax Description	<i>guest_lan_id</i>	Guest LAN identifier from 1 to 5 (inclusive).
	<i>interface_name</i>	Interface 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 provide a path between the wired guest client and the controller with guest LAN ID 1 and the interface name guest01:

```
(Cisco Controller) > config guest-lan ingress-interface 1 guest01
```

Related Commands	config interface guest-lan
	config guest-lan create

config guest-lan interface

To configure an egress interface to transmit wired guest traffic out of the controller, use the **config guest-lan interface** command.

config guest-lan interface *guest_lan_id* *interface_name*

Syntax Description	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
	<i>interface_name</i>	Interface 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 egress interface to transmit guest traffic out of the controller for guest LAN ID 1 and interface name guest01:

(Cisco Controller) > **config guest-lan interface 1 guest01**

Related Commands

config ingress-interface guest-lan

config guest-lan create

config guest-lan mobility anchor

To add or delete mobility anchor, use the **config guest-lan mobility anchor** command.

config guest-lan mobility anchor {**add** | **delete**} *Guest LAN Id IP addr*

Syntax Description	add	Adds a mobility anchor to a WLAN.
	delete	Deletes a mobility anchor from a WLAN.
	<i>Guest LAN Id</i>	Guest LAN identifier between 1 and 5.
	<i>IP addr</i>	Member switch IPv4 or IPv6 address to anchor 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 both IPv4 and IPv6 address formats.

The following example shows how to delete a mobility anchor for WAN ID 4 and the anchor IP 192.168.0.14:

```
(Cisco Controller) > config guest-lan mobility anchor delete 4 192.168.0.14
```

config guest-lan nac

To enable or disable Network Admission Control (NAC) out-of-band support for a guest LAN, use the **config guest-lan nac** command:

```
config guest-lan nac {enable | disable} guest_lan_id
```

Syntax Description	enable	Enables the NAC out-of-band support.
	disable	Disables the NAC out-of-band support.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).

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 NAC out-of-band support for guest LAN ID 3:

```
(Cisco Controller) > config guest-lan nac enable 3
```

Related Commands	show nac statistics
	show nac summary
	config wlan nac
	debug nac

config guest-lan security

To configure the security policy for the wired guest LAN, use the **config guest-lan security** command.

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

Syntax Description	web-auth	Specifies web authentication.
	enable	Enables the web authentication settings.
	disable	Disables the web authentication settings.
	acl	Configures an access control list.
	server-precedence	Configures the authentication server precedence order for web authentication users.
	<i>guest_lan_id</i>	LAN identifier between 1 and 5 (inclusive).
	web-passthrough	Specifies the web captive portal with no authentication required.
	email-input	Configures the web captive portal using an e-mail address.

Command Default	The default security policy for the wired guest LAN is web authentication.
------------------------	--

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 security web authentication policy for guest LAN ID 1:

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

Related Commands	config ingress-interface guest-lan config guest-lan create config interface guest-lan
-------------------------	--

config interface 3g-vlan

To configure 3G/4G-VLAN interface, use the **config interface 3g-vlan** command.

config interface 3g-vlan *interface-name* {**enable** | **disable**}

Syntax Description	<i>interface-name</i> enable	Enables the specified 3G/4G-VLAN interface
	<i>interface-name</i> disable	Disables the specified 3G/4G-VLAN interface

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

Command History	Release	Modification
	8.1	This command was introduced.

The following example shows how to configure 3G/4G-VLAN interface,:

(Cisco Controller) > **config interface 3g-vlan vlan-int enable**

config interface acl

To configure access control list of an interface, use the **config interface acl** command.

```
config interface acl { ap-manager | management | interface_name } {ACL | none }
```

Syntax Description	ap-manager	Configures the access point manager interface.
	management	Configures the management interface.
	interface_name	Interface name.
	ACL	ACL name up to 32 alphanumeric characters.
	none	Specifies none.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.</p> <p>The following example shows how to configure an access control list with a value None:</p> <pre>(Cisco Controller) > config interface acl management none</pre>	

config interface address

To configure address information for an interface, use the **config interface address** command.

config interface address { **ap-manager** *IP_address netmask gateway* | **management** *IP_address netmask gateway* | **service-port** *IP_address netmask* | **virtual** *IP_address* | **dynamic-interface** *IP_address dynamic_interface netmask gateway* | **redundancy-management** *IP_address* **peer-redundancy-management** *IP_address* }

Syntax Description	ap-manager	Specifies the access point manager interface.
	<i>IP_address</i>	IP address— IPv4 only.
	<i>netmask</i>	Network mask.
	<i>gateway</i>	IP address of the gateway.
	management	Specifies the management interface.
	service-port	Specifies the out-of-band service port interface.
	virtual	Specifies the virtual gateway interface.
	interface-name	Specifies the interface identified by the <i>interface-name</i> parameter.
	<i>interface-name</i>	Interface name.
	redundancy-management	Configures redundancy management interface IP address.
	peer-redundancy-management	Configures the peer redundancy management interface IP address.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	For Cisco 5500 Series Controllers, you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.	
	This command is applicable for IPv4 addresses only.	
	Ensure that the management interfaces of both controllers are in the same subnet. Ensure that the Redundant Management IP address for both controllers is the same. Likewise, ensure that the Peer Redundant Management IP address for both the controllers is the same.	
	The following example shows how to configure an access point manager interface with IP address 209.165.201.31, network mask 255.255.0.0, and gateway address 209.165.201.30:	

```
(Cisco Controller) > config interface address ap-manager 209.165.201.31 255.255.0.0  
209.165.201.30
```

The following example shows how to configure a redundancy management interface on the controller:

```
(Cisco Controller) > config interface address redundancy-management 209.4.120.5  
peer-redundancy-management 209.4.120.6
```

The following example shows how to configure a virtual interface:

```
(Cisco Controller) > config interface address virtual 192.0.2.1
```

Related Commands **show interface**

config interface address redundancy-management

To configure the management interface IP address, subnet and gateway of the controller, use the **config interface address redundancy-management** command.

config interface address redundancy-management *IP_address netmask gateway*

Syntax Description	<i>IP_address</i>	Management interface IP address of the active controller.
	<i>netmask</i>	Network mask.
	<i>gateway</i>	IP address of the gateway.
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 this command to check the Active-Standby reachability when the keep-alive fails.

The following example shows how to configure the management IP addresses of the controller:

```
(Cisco Controller) > config interface address redundancy-management 209.165.201.31 255.255.0.0 209.165.201.30
```

Related Commands

- config redundancy mobilitymac**
- config redundancy interface address peer-service-port**
- config redundancy peer-route**
- config redundancy unit**
- config redundancy timer**
- show redundancy timers**
- show redundancy summary**
- debug rmgr**
- debug rsyncmgr**

config interface ap-manager

To enable or disable access point manager features on the management or dynamic interface, use the **config interface ap-manager** command.

config interface ap-manager { **management** | *interface_name* } { **enable** | **disable** }

Syntax Description	management	Specifies the management interface.
	<i>interface_name</i>	Dynamic interface name.
	enable	Enables access point manager features on a dynamic interface.
	disable	Disables access point manager features on a dynamic interface.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use the **management** option to enable or disable dynamic AP management for the management interface. For Cisco 5500 Series Controllers, the management interface acts like an AP-manager interface by default. If desired, you can disable the management interface as an AP-manager interface and create another dynamic interface as an AP manager.

When you enable this feature for a dynamic interface, the dynamic interface is configured as an AP-manager interface (only one AP-manager interface is allowed per physical port). A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

The following example shows how to disable an access point manager myinterface:

```
(Cisco Controller) > config interface ap-manager myinterface disable
```

config interface create

To create a dynamic interface (VLAN) for wired guest user access, use the **config interface create** command.

config interface create *interface_name* *vlan-id*

Syntax Description	<i>interface_name</i>	Interface name.
	<i>vlan-id</i>	VLAN 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 create a dynamic interface with the interface named lab2 and VLAN ID 6:

```
(Cisco Controller) > config interface create lab2 6
```


config interface delete

To delete a dynamic interface, use the **config interface delete** command.

config interface delete *interface-name*

Syntax Description	<i>interface-name</i>	<i>interface-name</i> Interface 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 delete a dynamic interface named VLAN501:

```
(Cisco Controller) > config interface delete VLAN501
```

config interface dhcp management

To configure DHCP options on a management interface, use the **config interface dhcp management** command.

```
config interface dhcp management {option-82 {bridge-mode-insertion {enable | disable} |
enable | disable | linksel {enable | disable | relaysrc interface-name} | vpnsel {enable |
disable | vpnid vpn-id | vrfname vrf-name}} | primary primary-dhcp_server [ secondary
secondary-dhcp_server ] | proxy-mode {enable | disable | global} }
```

Syntax Description

option-82	Configures DHCP Option 82 on the interface.
bridge-mode-insertion	Configures DHCP option 82 insertion in bridge mode.
disable	Disables the feature.
enable	Enables the feature.
linksel	Configures link select suboption 5 on a dynamic or management interface.
relaysrc	Configures Link select suboption 5 on relay source.
<i>interface-name</i>	Name of an existing controller interface reachable from the DHCP server.
vpnid	Configures VPN select suboption 151 VPN Id.
<i>vpn-id</i>	VPN Id in oui:vpn-index format xxxxxx:xxxxxxxx.
vrfname	Configures VPN select suboption 151 VRF name.
<i>vrf-name</i>	VRF name as string of length 7.
primary	Specifies the primary DHCP server.
<i>primary-dhcp-server</i>	IP address of the server.
secondary	(Optional) Specifies the secondary DHCP server.
<i>secondary-dhcp-server</i>	IP address of the server.
proxy-mode	Configures the DHCP proxy mode on the interface.
global	Uses the global DHCP proxy mode on the interface.
disable	(Optional) Disables the DHCP proxy mode on the interface.
global	(Optional) Uses the global DHCP proxy mode on the interface.

Command Default

None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	The new keywords linksel and vpnsel are added. This command supports IPv6 from this release.

Usage Guidelines

DHCP proxy is not supported for IPv6 and it works in disabled mode.

The following example shows how to configure option 82 on a management interface.

```
(Cisco Controller) > config interface dhcp management option-82 enable
```

Related Commands

- config dhcp**
- config dhcp proxy**
- config interface dhcp**
- config wlan dhcp_server**
- debug dhcp**
- debug dhcp service-port**
- debug disable-all**
- show dhcp**
- show dhcp proxy**
- show interface**

config interface dhcp

Configure DHCP Option 82 insertion in Bridge mode on either management interface or dynamic interface by entering the **config interface dhcp** command:

```
config interface dhcp { management | dynamic-interface dynamic-interface-name } option-82  
bridge-mode-insertion { enable | disable }
```

Syntax Description

management	Management interface
dynamic-interface	Dynamic interface
<i>dynamic-interface-name</i>	Dynamic interface name
option-82	DHCP Option 82 on the interface
bridge-mode-insertion	To configure Bridge mode insertion

Command Default

DHCP option 82 insertion in Bridge mode is disabled.

Command History

Release	Modification
8.0	The Bridge mode insertion parameter was introduced in this release.

config interface dhcp dynamic-interface

To configure the DHCP option 6 override on the interface to use OpenDNS server IPs or not, use the **config interface dhcp dynamic-interface** command.

config interface dhcp dynamic-interface *intf-name* **option-6-opensns** { **enable** | **disable** }

Syntax Description	<i>intf-name</i>	Interface name.
	enable	Enables the DHCP option 6 override on the interface with OpenDNS IP address as default.
	disable	Disables the DHCP option 6 override on the interface and DHCP provided DNS IPs will be used..
Command Default	None	
Command Modes	Controller Config >	
Command History	Release	Modification
	8.4	This command was introduced.
Usage Guidelines	None	

Example

The following example shows how to configure the DHCP option 6 override on the interface to use OpenDNS server IPs:

```
(Cisco Controller) > config interface dhcp management option-6-opensns enable
```

config interface dhcp management option-6-opensns

To configure the DHCP Option 6 override on the interface in order to use OpenDNS server IPs, use the **config interface dhcp management option-6-opensns** command.

config interface dhcp management option-6-opensns { **enable** | **disable** }

Syntax Description	enable Enables the DHCP Option 6 override on the interface, with the OpenDNS IP address as the default.
	disable Disables the DHCP Option 6 override on the interface, and uses the DHCP-provided DNS IPs.
Command Default	DHCP Option 6 override is not enabled.
Command Modes	(Controller Configuration) >
Command History	Release Modification
	8.4 This command was introduced.

Example

The following example shows how to configure the DHCP Option 6 override on the interface in order to use OpenDNS server IPs:

```
(Cisco Controller) > config interface dhcp management option-6-opensns enable
```

config interface address

To configure interface addresses, use the **config interface address** command.

```
config interface address { dynamic-interface dynamic_interface netmask gateway | management |  
redundancy-management IP_address peer-redundancy-management | service-port netmask | virtual }  
IP_address
```

Syntax Description	dynamic-interface	Configures the dynamic interface of the controller.
	<i>dynamic_interface</i>	Dynamic interface of the controller.
	<i>IP_address</i>	IP address of the interface.
	<i>netmask</i>	Netmask of the interface.
	<i>gateway</i>	Gateway of the interface.
	management	Configures the management interface IP address.
	redundancy-management	Configures redundancy management interface IP address.
	peer-redundancy-management	Configures the peer redundancy management interface IP address.
	service-port	Configures the out-of-band service port.
	virtual	Configures the virtual gateway interface.

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 the management interfaces of both controllers are in the same subnet. Ensure that the redundant management IP address for both controllers is the same and that the peer redundant management IP address for both the controllers is the same.

The following example shows how to configure a redundancy management interface on the controller:

```
(Cisco Controller) >config interface address redundancy-management 209.4.120.5  
peer-redundancy-management 209.4.120.6
```

The following example shows how to configure a virtual interface:

```
(Cisco Controller) > config interface address virtual 10.10.10.1
```

config interface address

Related Commands show interface group summary
 show interface summary

config interface group failure-detect

To configure failure detection mode for an interface group, use the **config interface group failure-detect** command.

config interface group failure-detect *interface group name* { **aggressive** | **non-aggressive** }

Syntax Description	<i>interface-group-name</i>	Name of the interface group to enable the failure-detect mode. The interface group name can be up to 32 case-sensitive, alphanumeric characters.
	aggressive	The interface is marked as dirty if a client fails to get an IP from the DHCP server on this VLAN.
	non-aggressive	The interface is marked as dirty if a minimum of 3 different clients fail to get an IP on this VLAN.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	None	

The following example shows how to enable failure-detect, aggressive mode for an interface group floor1:

```
(Cisco Controller) > config interface group failure-detect floor1 aggressive
```

config interface group mdns-profile

To configure an mDNS (multicast DNS) profile for an interface group, use the **config interface group mdns-profile** command.

config interface group mdns-profile { **all** | *interface-group-name* } { *profile-name* | **none** }

Syntax Description	all	Configures an mDNS profile for all interface groups.
	<i>interface-group-name</i>	Name of the interface group to which the mDNS profile has to be associated. The interface group name can be up to 32 case-sensitive, alphanumeric characters.
	<i>profile-name</i>	Name of the mDNS profile.
	none	Removes all existing mDNS profiles from the interface group. You cannot configure mDNS profiles on the interface group.

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

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

Usage Guidelines If the mDNS profile is associated to a WLAN, an error appears.

The following example shows how to configure an mDNS profile for an interface group floor1:

```
(Cisco Controller) > config interface group mdns-profile floor1 profile1
```

Related Commands	config mdns query interval config mdns service config mdns snooping config interface mdns-profile config mdns profile config wlan mdns show mdns profile show mnds service clear mdns service-database debug mdns all debug mdns error debug mdns detail debug mdns message
------------------	--

config interface guest-lan

To enable or disable the guest LAN VLAN, use the **config interface guest-lan** command.

```
config interface guest-lan interface_name {enable | disable}
```

Syntax Description	interface_name	Interface name.
	enable	Enables the guest LAN.
	disable	Disables the guest 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 the guest LAN feature on the interface named myinterface:

```
(Cisco Controller) > config interface guest-lan myinterface enable
```

Related Commands	config guest-lan create
------------------	-------------------------

config interface hostname

To configure the Domain Name System (DNS) hostname of the virtual gateway interface, use the **config interface hostname** command.

config interface hostname virtual *DNS_host*

Syntax Description	virtual	Specifies the virtual gateway interface to use the specified virtual address of the fully qualified DNS name. The virtual gateway IP address is any fictitious, unassigned IP address, such as 192.0.2.1, to be used by Layer 3 security and mobility managers.
	<i>DNS_host</i>	DNS hostname.
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 virtual gateway interface to use the specified virtual address of the fully qualified DNS hostname DNS_Host:

```
(Cisco Controller) > config interface hostname virtual DNS_Host
```

config interface nasid

To configure the Network Access Server identifier (NAS-ID) for the interface, use the **config interface nasid** command.

config interface nasid {*NAS-ID* | **none**} *interface_name*

Syntax Description	<i>NAS-ID</i>	Network Access Server identifier (NAS-ID) for the interface. 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.
	none	Configures the controller system name as the NAS-ID.
	<i>interface_name</i>	Interface 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.
Usage Guidelines	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 configure the NAS-ID for the interface: (Cisco Controller) > config interface nasid	
Related Commands	config wlan nasid	
	config wlan apgroup	

config interface nat-address

To deploy your Cisco 5500 Series Controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT), use the **config interface nat-address** command.

```
config interface nat-address {management | dynamic-interface interface_name} {{enable | disable} | {set public_IP_address}}
```

Syntax Description	management	Specifies the management interface.
	dynamic-interface <i>interface_name</i>	Specifies the dynamic interface name.
	enable	Enables one-to-one mapping NAT on the interface.
	disable	Disables one-to-one mapping NAT on the interface.
	<i>public_IP_address</i>	External NAT IP address.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	These NAT commands can be used only on Cisco 5500 Series Controllers and only if the management interface is configured for dynamic AP management.	
	These commands are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. They do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.	
	The following example shows how to enable one-to-one mapping NAT on the management interface:	
	<pre>(Cisco Controller) > config interface nat-address management enable</pre>	
	The following example shows how to set the external NAT IP address 10.10.10.10 on the management interface:	
<pre>(Cisco Controller) > config interface nat-address management set 10.10.10.10</pre>		

config interface port

To map a physical port to the interface (if a link aggregation trunk is not configured), use the **config interface port** command.

config interface port { **management** | *interface_name* | **redundancy-management** } *primary_port* [*secondary_port*]

Syntax Description	management	Specifies the management interface.
	<i>interface_name</i>	Interface name.
	redundancy-management	Specifies the redundancy management interface.
	<i>primary_port</i>	Primary physical port number.
	<i>secondary_port</i>	(Optional) Secondary physical port number.

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 **management** option for all controllers except the Cisco 5500 Series Controllers.

The following example shows how to configure the primary port number of the LAb02 interface to 3:

```
(Cisco Controller) > config interface port lab02 3
```

config interface quarantine vlan

To configure a quarantine VLAN on any dynamic interface, use the **config interface quarantine vlan** command.

config interface quarantine vlan *interface-name* *vlan_id*

Syntax Description	<i>interface-name</i>	Interface's name.
	<i>vlan_id</i>	VLAN identifier.
	Note Enter 0 to disable quarantine processing.	
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 quarantine VLAN on the quarantine interface with the VLAN ID 10:

```
(Cisco Controller) > config interface quarantine vlan quarantine 10
```


config interface url-acl

To Configures an interface's URL Access Control List, use the **config interface url-acl** command.

```
config interface url-acl { management | interface_name } { acl-name | none }
```

Syntax Description	management	Configures the management interface.
	interface_name	Interface name.
	acl-name	ACL name up to 32 alphanumeric characters.
	none	Disable the acl configured on the interface.
Command Default	None	
Command History	Release	Modification
	8.3	This command was introduced.

This example shows how to configure an interface's url acl:

```
(Cisco Controller) >config interface url-acl management test
```

config interface vlan

To configure an interface VLAN identifier, use the **config interface vlan** command.

```
config interface vlan {ap-manager | management | interface-name | redundancy-management}
vlan
```

Syntax Description	ap-manager	Configures the access point manager interface.
	management	Configures the management interface.
	interface_name	Interface name.
	vlan	VLAN identifier.
	redundancy-management	Specifies the redundancy management interface.
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 change the redundancy management VLAN when the system redundancy management interface is mapped to the redundancy port. You must configure the redundancy management port first.	

The following example shows how to configure VLAN ID 10 on the management interface:

```
(Cisco Controller) > config interface vlan management 10
```

config interface mdns-profile

To configure an mDNS (multicast DNS) profile for an interface, use the **config interface mdns-profile** command.

config interface mdns-profile { **management** | **all** *interface-name* } { *profile-name* | **none** }

Syntax Description	management	Configures an mDNS profile for the management interface.
	all	Configures an mDNS profile for all interfaces.
	<i>interface-name</i>	Name of the interface on which the mDNS profile has to be configured. The interface name can be up to 32 case-sensitive, alphanumeric characters.
	<i>profile-name</i>	Name of the mDNS profile.
	none	Removes all existing mDNS profiles from the interface. You cannot configure mDNS profiles on the interface.

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

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

Usage Guidelines If the mDNS profile is associated to a WLAN, an error appears.

The following example shows how to configure an mDNS profile for an interface lab1:

```
(Cisco Controller) > config interface mdns-profile lab1 profile1
```

Related Commands	config mdns query interval
	config mdns service
	config mdns snooping
	config mdns profile
	config interface group mdns-profile
	config wlan mdns
	show mdns profile
	show mnds service
	clear mdns service-database
	debug mdns all
	debug mdns error
	debug mdns detail

debug mdns message

config icons delete

To delete an icon or icons from flash, use the **config icons delete** command in the WLAN configuration mode.

```
config icons delete { filename | all }
```

Syntax Description	<i>filename</i>	Name of the icon to be deleted.
	all	Deletes all the icon files from the system.
Command Default	None	
Command Modes	WLAN configuration	
Command History	Release	Modification
	Release 8.2	This command was introduced.

The following example shows how to delete an icon from flash:

```
Cisco Controller > config icons delete image-1
```

config icons file-info

To configure an icon parameter, use the **config icons file-info** command in WLAN configuration mode.

config icons file-info *filename file-type lang-code width height*

Syntax Description

<i>filename</i>	Icon filename. It can be up to 32 characters long.
<i>file-type</i>	Icon filename type or extension. It can be up to 32 characters long.
<i>lang-code</i>	Language code of the icon. Enter 2 or 3 letters from ISO-639, for example: <i>eng</i> for English.
<i>width</i>	Icon width. The range is from 1 to 65535.
<i>height</i>	Icon height. The range is from 1 to 65535.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure icon parameters:

```
Cisco Controller > config icons file-info ima png eng 300 200
```

config ipv6 disable

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

config ipv6 disable

Syntax Description	This command has no arguments or keywords.	
Command Default	By default, the IPv6 configuration is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>When you use this command, the controller drops all IPv6 packets and the clients will not receive any IPv6 address.</p> <p>The following example shows how to disable IPv6 on the controller:</p> <pre>(Cisco Controller) >config ipv6 disable</pre>	

config ipv6 enable

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

config ipv6 enable

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

Command Default	By default, the IPv6 configuration 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 enable IPv6 on the controller:

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


config ipv6 acl

To create or delete an IPv6 ACL on the Cisco wireless LAN controller, apply ACL to data path, and configure rules in the IPv6 ACL, use the **config ipv6 acl** command.

```

config ipv6 acl [apply | cpu | create | delete | rule]
config ipv6 acl apply name
config ipv6 acl cpu {name | none}
config ipv6 acl create name
config ipv6 acl delete name
config ipv6 acl rule [action | add | change | delete | destination | direction | dscp | protocol
| source | swap ]
config ipv6 acl rule action name index {permit | deny}
config ipv6 acl rule add name index
config ipv6 acl rule change index name old_index new_index
config ipv6 acl rule delete name index
config ipv6 acl rule destination {address name index ip_address prefix-len | port range name index }
config ipv6 acl rule direction name index {in | out | any}
config ipv6 acl rule dscp name dscp
config ipv6 acl rule protocol name index protocol
config ipv6 acl rule source {address name index ip_address prefix-len | port range name index
start_port end_port}
config ipv6 acl rule swap index name index_1 index_2

```

Syntax Description		
apply <i>name</i>		Applies an IPv6 ACL. An IPv6 ACL can contain up to 32 alphanumeric characters.
cpu <i>name</i>		Applies the IPv6 ACL to the CPU.
cpu none		Configure none if you wish not to have a IPV6 ACL.
create		Creates an IPv6 ACL.
delete		Deletes an IPv6 ACL.
rule (action) (<i>name</i>) (<i>index</i>)		Configures rules in the IPv6 ACL to either permit or deny access. IPv6 ACL name can contains up to 32 alphanumeric characters and IPv6 ACL rule index can be between 1 and 32.
{ permit deny }		Permit or deny the IPv6 rule action.
add <i>name index</i>		Adds a new rule and rule index.
change <i>name old_index new_index</i>		Changes a rule's index.
delete <i>name index</i>		Deletes a rule and rule index.
destination address <i>name index ip_addr prefix-len</i>		Configures a rule's destination IP address and prefix length (between 0 and 128).

destination port <i>name index</i>	Configure a rule's destination port range. Enter IPv6 ACL name and set an rule index for it.
direction <i>name index</i> { in out any }	Configures a rule's direction to in, out, or any.
dscp <i>name index dscp</i>	Configures a rule's DSCP. For rule index of DSCP, select a number between 0 and 63, or any .
protocol <i>name index protocol</i>	Configures a rule's protocol. Enter a name and set an index between 0 and 255 or any .
source address <i>name index</i> <i>ip_address prefix-len</i>	Configures a rule's source IP address and netmask.
source port range <i>name index</i> <i>start_port end_port</i>	Configures a rule's source port range.
swap index <i>name index_1</i> <i>index_2</i>	Swap's two rules' indices.

Command Default

After adding an ACL, the **config ipv6 acl cpu** is by default configured as **enabled**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6..
8.0	This command was updated by adding cpu and none keywords and the <i>ipv6_acl_name</i> variable.

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to configure an IPv6 ACL to permit access:

```
(Cisco Controller) >config ipv6 acl rule action lab1 4 permit
```

The following example shows how to configure an interface ACL:

```
(Cisco Controller) > config ipv6 interface acl management IPv6-Acl
```

Related Commands

show ipv6 acl detailed
show ipv6 acl cpu

config ipv6 capwap

To enable or disable an IPv6 CAPWAP UDPLite for CAPWAP AP on the controller, use the **config ipv6 capwap** command.

config ipv6 capwap udplite { **enable** | **disable** } [**all** | *cisco-ap*]

Syntax Description	udplite	Configure IPv6 for CAPWAP UDP Lite.
	enable	Enables IPv6 CAPWAP UDP Lite.
	disable	Disables IPv6 CAPWAP UDP Lite.
	all	Enables or disables IPv6 CAPWAP UDP Lite on all Cisco APs.
	<i>cisco-ap</i>	Enables or disables IPv6 CAPWAP UDP Lite on the user defined Cisco AP.

Command Default The **config ipv6 capwap udplite** command is by default configured as **enabled**.

Command History	Release	Modification
	8.0	This command was introduced in Release 8.0

- Usage Guidelines**
- IPv6 CAPWAP UDP Lite configuration applies only to APs that are connected to controller using IPv6 tunnel.
 - For APs connected to controller using IPv4 Tunnel, IPv6 CAPWAP UDPLite command will not apply on either global configuration or on Per AP.
 - IPv6 mandates complete payload checksum for UDP and this will have performance implications. To minimize the impact, UDPLite (mandates only header checksum) will be used for data traffic and UDP for control traffic.
 - Usage UDP Lite will have an impact on the firewall. Intermediate firewall must be configured to allow UDP Lite protocol (protocol ID of 136) packets.
 - Turning off UDP Lite will cause performance issues on packet handling.
 - Changing from UDP to UDPLite or vice-versa will enforce the AP to disjoin and re-join.

The following example shows how to configure an IPv6 CAPWAP UDP Lite on All Cisco APs or on a particular Cisco AP:

```
(Cisco Controller) >config ipv6 capwap udplite enable all
Changing AP's IPv6 Capwap UDP Lite mode will cause the AP to rejoin.
Are you sure you want to continue? (y/n)
```

config ipv6 interface

To configure IPv6 system interfaces, use the **config ipv6 interface** command.

config ipv6 interface { **acl** | **address** | **slaac** }

config ipv6 interface acl management *acl_name*

config ipv6 interface address { **management primary** *ipv6_address prefix_length ipv6_gateway_address* | **service-port** *ipv6_address prefix-length* }

config ipv6 interface slacc service-port [**enable** | **disable**]

Syntax	Description
acl	Configures IPv6 on an interface's Access Control List.
management	Configures the management interface.
<i>acl_name</i>	Enter IPv6 ACL name for the management ACL. It supports up to 32 alphanumeric characters.
address	Configures IPv6 on an interface's address information.
management	Configures the management interface.
primary	Configures the primary IPv6 Address for an interface
<i>ipv6_address</i>	Configures an interface with IPv6 address information.
<i>prefix_length</i>	Configures IPv6 Prefix length. The range for prefix length is 1 to 127.
<i>ipv6_gateway_address</i>	Configures the Link Layer IPv6 gateway Address.
service-port	Configures IPv6 on the out-of-band service Port.
<i>ipv6_address</i>	Configures an interface with IPv6 address information.
<i>prefix_length</i>	Configures IPv6 Prefix length. The range for prefix length is 1 to 127.
slacc	Configures SLAAC options on an interface.
service-port	Configures IPv6 on the out-of-band service Port.
enable	Enables SLAAC Option
disable	Disables SLAAC Option
Command Default	None.

Command History	Release	Modification
	8.0	This command was introduced in Release 8.0.

The following example shows how to configure an IPv6 ACL management interface:

```
(Cisco Controller) >config ipv6 interface acl management Test_ACL
```

The following example shows how to configure an IPv6 address and primary interface:

```
(Cisco Controller) > config ipv6 interface address management primary 2001:9:10:56::44 64  
fe80::aea0:16ff:fe4f:2244
```

Related Commands	show interface detailed management
	show ipv6 interface summary

config ipv6 multicast

To configure IPv6 multicast, use the **config ipv6 multicast** command.

config ipv6 multicast mode { **unicast** | **multicast** *ipv6_address* }

Syntax Description

mode	Configure the controller to AP Multicast or Broadcast IPv6 traffic forwarding mode.
unicast	Multicast/Broadcast IPv6 packets are encapsulated in unicast CAPWAP tunnel to AP.
multicast	Multicast/Broadcast IPv6 packets are encapsulated in multicast CAPWAP tunnel to AP.
<i>ipv6_address</i>	Configures IPv6 multicast address.

Command Default

- By default, multicast is enabled on Cisco 8500 and 2500 Series Wireless Controllers.
- By default, unicast is enabled on Cisco 5500 Series Wireless Controllers.

Command History

Release	Modification
8.0	This command was introduced in Release 8.0.

Usage Guidelines

none...

The following example shows how to configure an IPv6 multicast on the controller, to permit access:

```
(Cisco Controller) >config ipv6 multicast 2001:DB8:0000:0000:0000:0000:0000:0001
```

The following example shows how to configure an IPv6 unicast on the controller, to permit access:

```
(Cisco Controller) > config ipv6 multicast mode unicast
```

Related Commands

show network summary

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
timers	Configures the neighbor binding table timeout timers.
down-lifetime	Configures the down lifetime.
<i>down_time</i>	Down lifetime in seconds. The range is from 0 to 86400. The default is 30 seconds.
reachable-lifetime	Configures the reachable lifetime.
<i>reachable_time</i>	Reachable lifetime in seconds. The range is from 0 to 86400. The default is 300 seconds.
stale-lifetime	Configures the stale lifetime.
<i>stale_time</i>	Stale lifetime in seconds. The range is from 0 to 86400. The default is 86400 seconds.
ra-throttle	Configures IPv6 RA throttling options.
allow	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.
enable	Enables IPv6 RA throttling.
disable	Disables IPv6 RA throttling.
interval-option	Adjusts the behavior on RA with RFC3775 interval option.
ignore	Indicates interval option has no influence on throttling.
passthrough	Indicates all RAs with RFC3775 interval option will be forwarded (default).
throttle	Indicates all RAs with RFC3775 interval option will be throttled.

max-through	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.
no-limit	Configures no upper bound at the VLAN level.
throttle-period	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.

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 Neighbor Binding table:

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

Related Commands **show ipv6 neighbor-binding**

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}
```

Syntax Description	enable	Enables nonstop multicast forwarding on a cache miss.
	disable	Disables nonstop multicast forwarding on a cache miss.
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 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	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 ipv6 route

To add or delete an IPv6 network route, use the **config ipv6 route** command.

config ipv6 route { **add** *network_ipv6_addr prefix-len ipv6_gw_addr* | **delete** *network_ipv6_addr* }

Syntax Description	add	Adds an IPv6 network route.
	<i>network_ipv6_addr</i>	Enter the networks IPv6 address.
	<i>prefix-len</i>	Enter the prefix length for the network.
	<i>ipv6_gw_addr</i>	Configures the system interfaces.
	delete	Deletes an IPv6 network route.
	<i>network_ipv6_addr</i>	Enter the networks IPv6 address.
Command Default	None	
Command History	Release	Modification
	8.0	This command was introduced in Release 8.0.
Usage Guidelines	<ul style="list-style-type: none"> This command is used to add and delete an IPv6 network route to access service interface over IPv6 from different network. While adding IPv6 route, IPv6 Gateway Address must be a link local scope (FE80::/64). <p>The following example shows how to add an IPv6 route:</p> <pre>(Cisco Controller) > config ipv6 route add 3010:1111:2222:abcd:abcd:abcd:abcd:1111 64 fe80::6616:8dff:fed3:c0cf</pre> <p>The following example shows how to delete an IPv6 route:</p> <pre>(Cisco Controller) > config ipv6 route delete 2001:9:5:90::115</pre>	
Related Commands	show ipv6 route summary	

